Nessus 4.4 Benutzerhandbuch

14. Juni 2011

(Revision 10)

Copyright © 2011 Tenable Network Security, Inc. Alle Rechte vorbehalten. Tenable Network Security und Nessus sind eingetragene Marken von Tenable Network Security, Inc. ProfessionalFeed ist eine Marke von Tenable Network Security, Inc. Alle anderen Produkte und Dienstleistungen sind Marken ihrer jeweiligen Eigentümer.

Tenable Network Security, Inc. • 7063 Columbia Gateway Drive, Suite 100, Columbia, MD 21046, USA • +1 410 872 0555 • sales@tenable.com • www.tenable.com

Inhaltsverzeichnis

Einleitung.. 3
Regeln und Konventionen 3

Die Nessus-Benutzeroberfläche im Überblick 3
Beschreibung 3
Unterstützte Plattformen 4

Installation. 4

Bedienung. 4
Übersicht 4
Verbindung mit der Nessus-Benutzeroberfläche herstellen 4
Überblick zu den Richtlinien 8
Standardrichtlinien 9
Neue Richtlinie erstellen 10
General 10
Credentials 15
Plugins 18
Preferences 21
Richtlinien importieren, exportieren und kopieren 39
Scans erstellen, starten und planen 40
Berichte 43
Browse (Durchsuchen) 44
Berichtsfilter 48
Compare (Vergleichen) 51
Upload und Download 52
Das .nessus-Dateiformat 54
Delete (Löschen) 55
Benutzer 55

Andere Nessus-Clients 55
Die Befehlszeilenoberfläche 55
Bericht konvertieren 57
.nessus-Dateien auf der Befehlszeile bearbeiten 58
Scanbefehl 59
SecurityCenter 60
SecurityCenter konfigurieren 60

Weitere Informationen 61

Wissenswertes zu Tenable Network Security 63

Copyright © 2002-2011 Tenable Network Security, Inc.

EINLEITUNG

Das vorliegende Dokument beschreibt die Verwendung der **Nessus-Benutzeroberfläche (UI)** von Tenable Network Security. Wir freuen uns über Ihre Anmerkungen und Vorschläge zu diesem Produkt. Schicken Sie einfach eine E-Mail an support@tenable.com.

Die Nessus-Benutzeroberfläche ist eine webbasierte Oberfläche für den Nessus-Sicherheitslückenscanner. Zur Verwendung des Clients muss ein betriebsbereiter Nessus-Scanner in Ihrer Umgebung vorhanden sein, und Sie müssen mit der Bedienung des Scanners vertraut sein.

REGELN UND KONVENTIONEN

Das vorliegende Dokument wurde aus einer ursprünglich auf Englisch verfassten Version übersetzt. Teilweise wurden Texte auf Englisch beibehalten, wenn diese in englischer Form im Produkt erscheinen.

In der gesamten Dokumentation werden Dateinamen, Daemons und ausführbare Dateien in einer Schriftart wie **`courier bold`** angezeigt (Beispiel: **`gunzip`**, **`httpd`** und **`/etc/passwd`**).

Befehlszeichenoptionen und Schlüsselwörter werden ebenfalls in der Schriftart **`courier bold`** angezeigt. Die Befehlszeilen sind teils mit, teils ohne Befehlszeilen-Prompt und den Ausgabetext des betreffenden Befehls aufgeführt. Häufig ist der Befehl **fett** gedruckt, um zu verdeutlichen, was der Benutzer eingegeben hat. Es folgt ein Beispiel für die Ausführung des UNIX-Befehls **`pwd`**:

```
# pwd
/opt/nessus/
#
```

Wichtige Hinweise und Aspekte werden durch dieses Symbol und graue Textfelder hervorgehoben.

Tipps, Beispiele und Best Practices (Empfehlungen) werden durch dieses Symbol und weißen Text auf blauem Grund hervorgehoben.

DIE NESSUS-BENUTZEROBERFLÄCHE IM ÜBERBLICK

BESCHREIBUNG

Die Nessus-Benutzeroberfläche (User Interface, UI) ist eine webbasierte Oberfläche für den Nessus-Scanner. Sie umfasst einen einfachen HTTP-Server und Webclient und erfordert abgesehen vom Nessus-Server keine weitere Softwareinstallation. Seit Nessus 4 weisen alle Plattformen dieselbe Codebasis auf. Hierdurch werden nicht nur die meisten plattformspezifischen Bugs und Fehler beseitigt, sondern auch eine schnellere Bereitstellung neuer Funktionen ermöglicht. Die wesentlichen Merkmale sind:

- Generierung von **`.nessus`**-Dateien, die von Tenable-Produkten standardmäßig als Grundlage für Informationen zu Sicherheitslücken und Scanrichtlinien verwendet werden.

Copyright © 2002-2011 Tenable Network Security, Inc.

- In einer einzigen `.nessus`-Datei lassen sich eine Richtliniensitzung, eine Liste mit Zielen und die Ergebnisse mehrerer Scans speichern und problemlos exportieren. Weitere Informationen entnehmen Sie dem Leitfaden zu den Nessus-Dateiformaten.
- Die Benutzeroberfläche zeigt Scanergebnisse in Echtzeit an. Sie müssen also nicht warten, bis ein Scan abgeschlossen ist, um die Resultate aufzurufen.
- Unabhängig von der Basisplattform wird eine einheitliche Oberfläche für den Nessus-Scanner bereitgestellt. Unter Mac OS X, Windows und Linux ist jeweils derselbe Leistungsumfang vorhanden.
- Die Ausführung von Scans auf dem Server wird nicht unterbrochen, wenn Ihre Verbindung aus irgendeinem Grund getrennt wird.
- Nessus-Scanberichte können über die Nessus-Benutzeroberfläche hochgeladen und mit anderen Berichten verglichen werden.

Unterstützte Plattformen

Da die Nessus-Benutzeroberfläche ein webbasierter Client ist, kann sie auf jeder Plattform ausgeführt werden, die einen Webbrowser bereitstellt.

Die webbasierte Nessus-Benutzeroberfläche bietet maximale Leistung bei Verwendung von Microsoft Internet Explorer 7 und 8, Mozilla Firefox 3.5.x und 3.6.x oder Apple Safari.

INSTALLATION

Seit Nessus 4.2 erfolgt die Benutzerverwaltung des Nessus-Servers über eine Weboberfläche oder SecurityCenter. Der vormals benötigte NessusClient wird hierzu nicht mehr eingesetzt. Der Scanner kann zwar weiterhin über den NessusClient bedient werden, es wird aber für den Client keine Updates mehr geben.

Weitere Informationen zur Installation von Nessus finden Sie im Nessus 4.4 Installationshandbuch. Die Installation zusätzlicher Software ist nicht erforderlich.

BEDIENUNG

Übersicht

Nessus stellt eine einfache, aber leistungsfähige Oberfläche zur Verwaltung der Scanaktivitäten bereit.

Verbindung mit der Nessus-Benutzeroberfläche herstellen

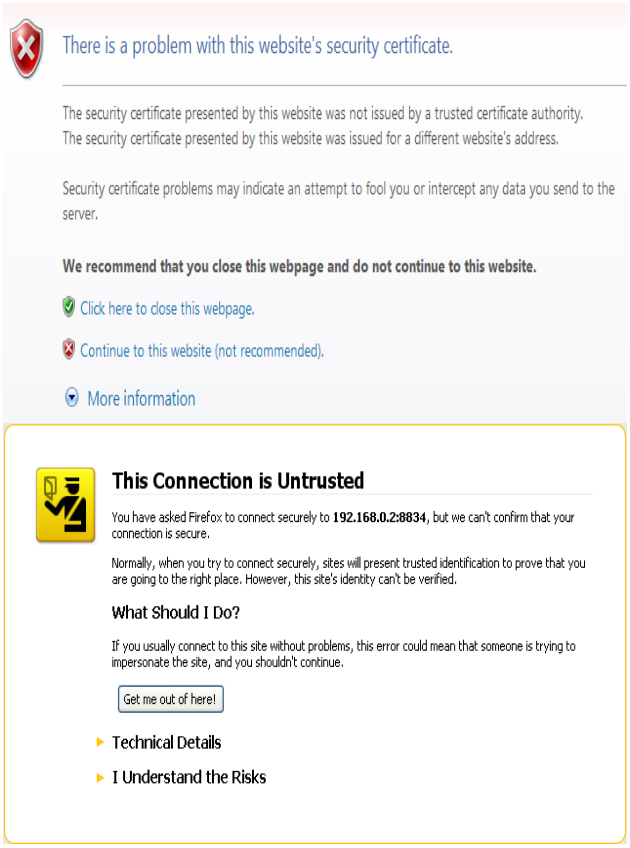
Führen Sie die folgenden Schritte aus, um die Nessus-Benutzeroberfläche zu starten:

- Öffnen Sie einen beliebigen Webbrowser.
- Geben Sie https://[Server-IP-Adresse]:8834/ in die Navigationsleiste ein.

Achten Sie in jedem Fall darauf, die Verbindung mit der Benutzeroberfläche über HTTPS herzustellen, da nicht verschlüsselte HTTP-Verbindungen nicht unterstützt werden.

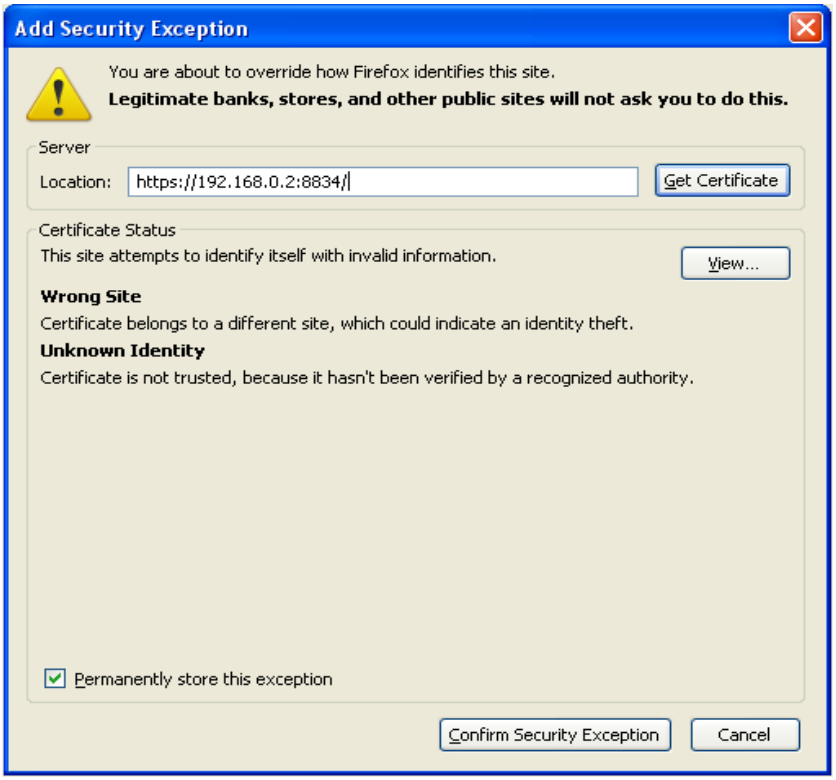
Copyright © 2002-2011 Tenable Network Security, Inc.

Wenn Sie zum ersten Mal eine Verbindung mit der Benutzeroberfläche des Nessus-Scanners herstellen, zeigen die meisten Webbrowser eine Fehlermeldung an, laut der die Website nicht vertrauenswürdig ist, weil das SSL-Zertifikat selbstsigniert ist:


There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information
This Connection is Untrusted
You have asked Firefox to connect securely to 192.168.0.2:8834, but we can't confirm that your connection is secure.
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.
What Should I Do?
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.
Get me out of here!
Technical Details
I Understand the Risks

Benutzer von Microsoft Internet Explorer können auf „Laden dieser Website fortsetzen (nicht empfohlen)" klicken, um die Nessus-Benutzeroberfläche zu laden. Benutzer von Firefox 3.x klicken auf „Ich kenne das Risiko" und dann auf „Ausnahme hinzufügen…", um das Dialogfeld „Sicherheits-Ausnahmeregel hinzufügen" aufzurufen:

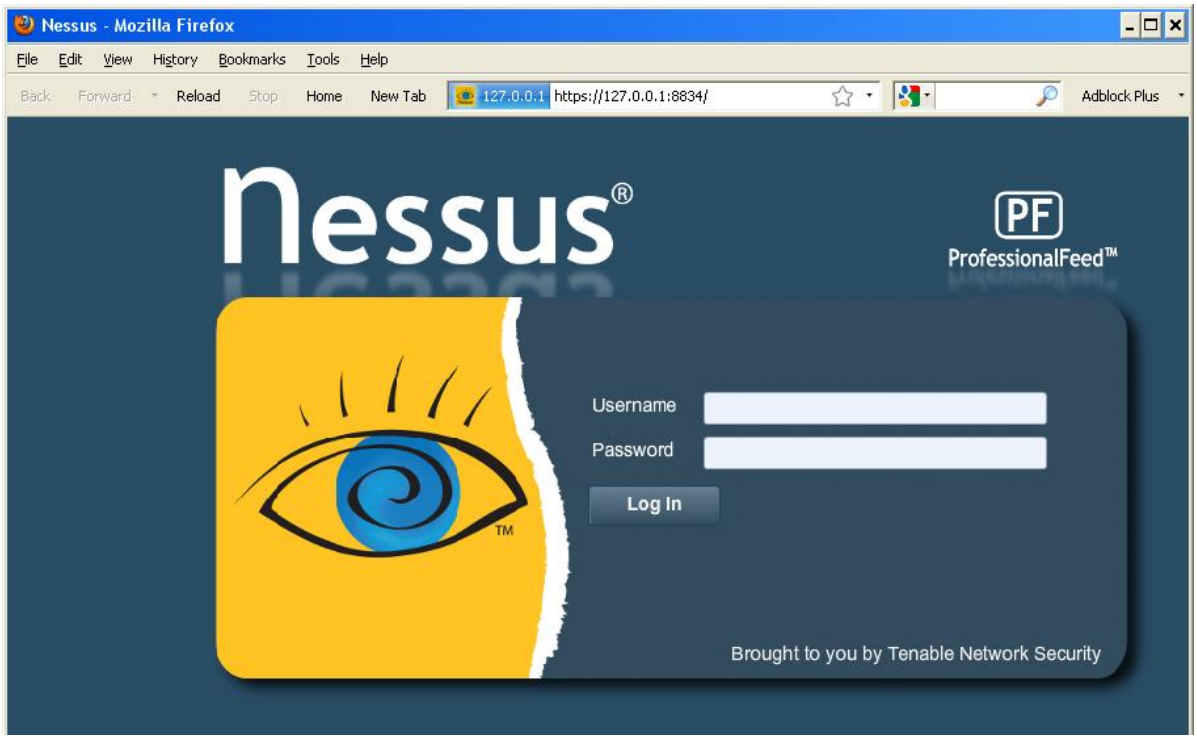
Copyright © 2002-2011 Tenable Network Security, Inc.


Add Security Exception
You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.
Server
Location: https://192.168.0.2:8834/
Get Certificate
Certificate Status
This site attempts to identify itself with invalid information.
View...
Wrong Site
Certificate belongs to a different site, which could indicate an identity theft.
Unknown Identity
Certificate is not trusted, because it hasn't been verified by a recognized authority.
Permanently store this exception
Confirm Security Exception
Cancel

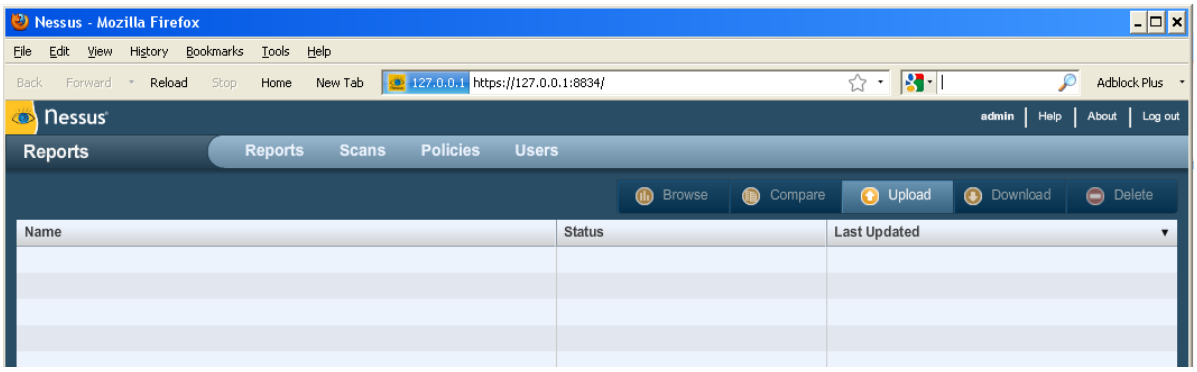
Vergewissern Sie sich, dass im Feld „Location" die URL des Nessus-Servers steht, und klicken Sie auf **„Confirm Security Exception"**. Weitere Informationen zur Installation eines angepassten SSL-Zertifikats entnehmen Sie dem Nessus-Installationshandbuch.

Copyright © 2002-2011 Tenable Network Security, Inc.

Nachdem die Ausnahme in Ihrem Browser bestätigt wurde, wird das folgende Startfenster angezeigt:

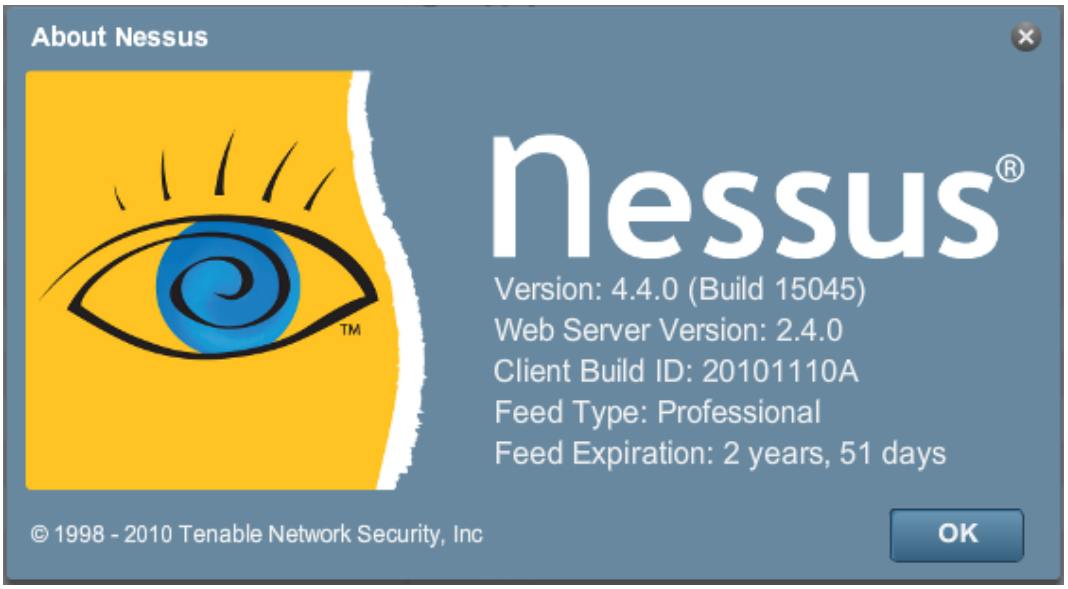


Authentifizieren Sie sich mithilfe des Benutzernamens und des Kennworts, das Sie zuvor mit dem Server Manager erstellt haben. Nach erfolgreicher Authentifizierung erscheinen auf der Benutzeroberfläche die Menüs zum Durchführen von Scans:


Nessus - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Back Forward Reload Stop Home New Tab 127.0.0.1 https://127.0.0.1:8834/ Adblock Plus
Nessus
admin Help About Log out
Reports
Reports Scans Policies Users
Browse Compare Upload Download Delete
Name Status Last Updated

Die oben rechts gezeigten Optionen sind zu jedem Zeitpunkt der Benutzung von Nessus verfügbar. Die Angabe „admin", die oben rechts in der oben gezeigten Abbildung zu sehen ist, nennt das Konto, unter dem Sie sich angemeldet haben. Wenn Sie darauf klicken, können Sie Ihr aktuelles Kennwort ändern. "„Help" („Hilfe") ist eine Verknüpfung mit der Nessus-Dokumentation, die ausführliche Hinweise zur Verwendung der Software enthält. "„About" („Info") zeigt wichtige Informationen zur Nessus-Installation an, z. B. die Version, Typ und Ablauf des Feeds, den Client-Build und die Webserverversion. „Log out" („Abmelden") beendet Ihre aktuelle Sitzung.

Copyright © 2002-2011 Tenable Network Security, Inc.



Überblick zu den Richtlinien

Eine Nessus-Richtlinie umfasst Konfigurationsoptionen für die Durchführung von Sicherheitslückenscans. Hierzu zählen unter anderem:

- Parameter zur Steuerung technischer Aspekte des Scans (z. B. Timeouts, Anzahl der Hosts, Art des Portscanners usw.)
- Anmeldedaten für lokale Scans (z. B. Windows, SSH), authentifizierte Oracle-Datenbankscans, HTTP, FTP, POP, IMAP, oder eine Kerberos-basierte Authentifizierung
- Spezifikationen für granulare familien- oder Plugin-basierte Scans
- Tests der Compliancerichtlinien für Datenbanken, Ausführlichkeit von Berichten, Scaneinstellungen für die Diensterkennung, UNIX-Compliancetests u. a.

Copyright © 2002-2011 Tenable Network Security, Inc.

STANDARDRICHTLINIEN

Nessus wird mit einer Reihe von Standardrichtlinien ausgeliefert, die von Tenable Network Security, Inc. bereitgestellt werden. Sie dienen einerseits als Vorlagen, auf deren Basis Sie angepasste Richtlinien für Ihre Organisation erstellen können, können aber auch direkt zur Ausführung einfacher Scans Ihrer Ressourcen verwendet werden.

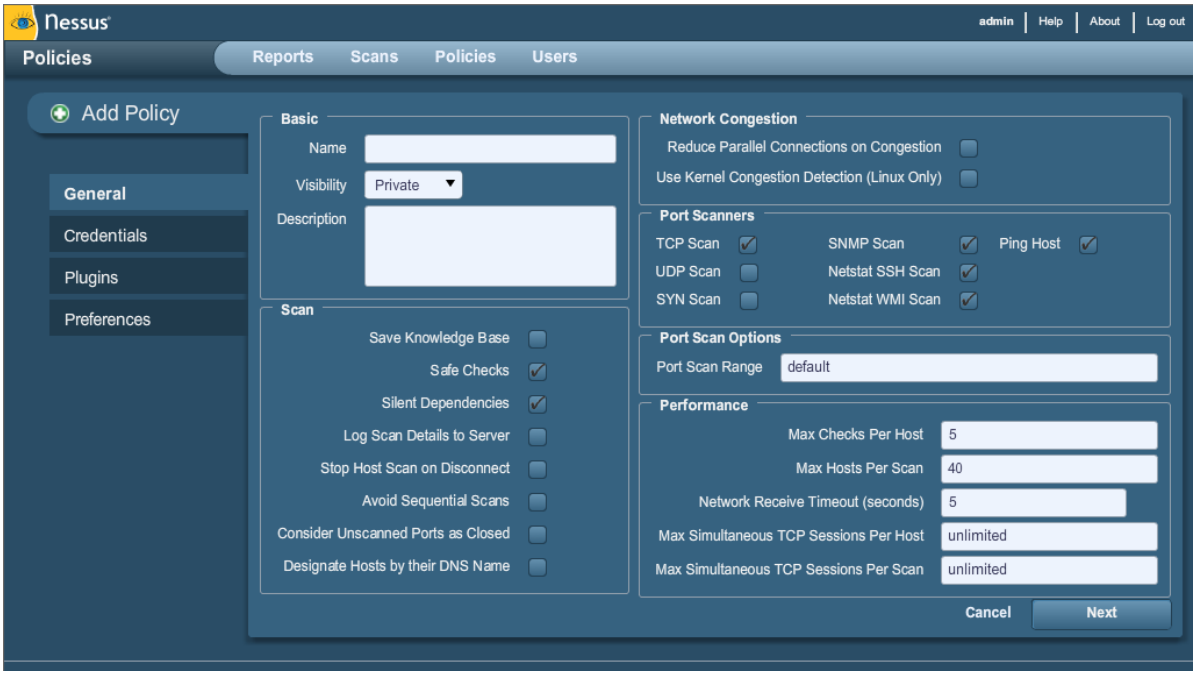
Name der Richtlinie	Beschreibung
External Network Scan	Diese Richtlinie dient dem Scannen von Hosts, die mit Ressourcen außerhalb Ihres Netzwerks verbunden sind. Solche Hosts stellen gewöhnlich weniger Dienste in Ihrem Netzwerk bereit. In dieser Richtlinie sind Plugins aktiviert, die bekannte Sicherheitslücken von Webanwendungen überprüfen (es sind dies die Plugin-Familien „CGI Abuses" und „CGI Abuses: XSS"). Außerdem werden alle 65.535 Ports auf jedem Ziel gescannt.
Internal Network Scan	Diese Richtlinie dient der Leistungsoptimierung. Bei der Erstellung wurde berücksichtigt, dass sie zum Scannen umfangreicher interner Netzwerke mit vielen Hosts, mehreren ungeschützten Diensten und eingebetteten Systemen wie etwa Druckern verwendet werden kann. Die „CGI Abuse"-Plugins sind hier nicht aktiviert, und es werden statt aller 65.535 nur häufig verwendete Ports gescannt.
Web App Tests	Wenn Sie Ihre Systeme scannen möchten und Nessus sowohl bekannte als auch unbekannte Sicherheitslücken in Ihren Webanwendungen erkennen soll, ist dies die passende Scanrichtlinie für Sie. Die unscharfen Suchfunktionen in Nessus sind in dieser Richtlinie aktiviert. Aufgrund dessen sucht Nessus auf allen erkannten Websites nach Sicherheitslücken in allen Parametern einschließlich XSS, SQL, Befehlsinjektion u. a.
Prepare for PCI DSS audits	Diese Richtlinie aktiviert die integrierten PCI-DSS-Compliancetests, bei denen Scanergebnisse mit den PCI-Standards verglichen werden und ein Bericht zum Complianceniveau erstellt wird. Es ist sehr wichtig festzuhalten, dass ein erfolgreicher Compliancescan weder Compliance noch eine sichere Infrastruktur garantiert. Organisationen, bei denen

Copyright © 2002-2011 Tenable Network Security, Inc.

	eine PCI-DSS-Bewertung ansteht, können ihr Netzwerk und ihre Systeme mithilfe dieser Richtlinie auf die PCI-DSS-Compliance vorbereiten.

NEUE RICHTLINIE ERSTELLEN

Wenn Sie eine Verbindung mit einer Nessus-Serverbenutzeroberfläche hergestellt haben, können Sie eine angepasste Richtlinie erstellen. Hierzu klicken Sie auf die Option „**Policies**" („Richtlinien") oben in der Menüleiste und dann rechts auf die Schaltfläche „**+ Add**" („Hinzufügen"). Das Fenster „**Add Policy**" („Richtlinie hinzufügen") erscheint:



Hier finden Sie vier Registerkarten für die Konfiguration: **General** („Allgemein"), **Credentials** („Anmeldedaten"), **Plugins** und **Preferences** („Einstellungen"). Die Standardeinstellungen ermöglichen eine maximal abgestufte Kontrolle des Nessus-Scannerbetriebs und müssen für die meisten Umgebungen nicht geändert werden. Die Registerkarten sind nachfolgend beschrieben.

General

Die Registerkarte General erlaubt das Benennen der Richtlinie und die Konfiguration scanspezifischer Vorgänge. Hier finden Sie sechs Bereiche mit zusammengefassten Optionen, die das Scannerverhalten steuern:

Im Bereich „**Basic**" („Grundlagen") definieren Sie Aspekte zur Richtlinie selbst:

Option	Beschreibung
Name	Hier wird der Name festgelegt, der zur Bezeichnung der Richtlinie auf der Nessus-Benutzeroberfläche verwendet wird.

Copyright © 2002-2011 Tenable Network Security, Inc.

Visibility (Sichtbarkeit)	Hierdurch wird bestimmt, ob die Richtlinie mit anderen Benutzern *gemeinsam verwendet* wird („Shared") oder Ihrem *persönlichen* Gebrauch vorbehalten bleibt („Private"). Nur Administratoren können Richtlinien zur gemeinsamen Verwendung freigeben.
Description (Beschreibung)	Hier kann eine kurze Beschreibung der Scanrichtlinie eingegeben werden. Das Feld eignet sich normalerweise zur Zusammenfassung des allgemeinen Zwecks der Richtlinie (z. B. „Webserverscans ohne lokale Tests und Nicht-HTTP-Dienste").

Im Bereich „**Scan**" werden die weiteren Optionen in Zusammenhang mit dem Verhalten eines Scans definiert:

Option	Beschreibung
Save Knowledge Base (Knowledge-Base speichern)	Der Nessus-Scanner kann Informationen zur späteren Verwendung in der Knowledge-Base (Informationsdatenbank) des Nessus-Servers speichern. Dies schließt offene Ports, erfolgreich ausgelöste Plugins, erkannte Dienste usw. ein.
Safe Checks (Sichere Tests)	„Safe Checks" deaktiviert alle Plugins, die sich unter Umständen negativ auf den Remotehost auswirken können.
Silent Dependencies (Abhängigkeiten nicht aufführen)	Wenn diese Option aktiviert ist, wird die Liste der Abhängigkeiten nicht im Bericht aufgeführt. Soll die Liste der Abhängigkeiten im Bericht enthalten sein, dann müssen Sie das Kontrollkästchen deaktivieren.
Log Scan Details to Server (Scandetails auf Server protokollieren)	Hiermit werden zusätzliche Details des Scans in die Nessus-Serverlogdatei (`nessusd.messages`) gespeichert, z. B. der Start, die Beendigung oder der erzwungene Abbruch von Plugins. Anhand der resultierenden Logdatei können Sie nachprüfen, ob bestimmte Plugins verwendet und Hosts gescannt wurden.
Stop Host Scan on Disconnect (Hostscan bei Trennung beenden)	Wenn diese Option aktiviert ist, beendet Nessus den Scan, sobald erkannt wurde, dass der Host nicht mehr reagiert. Dies kann beispielsweise geschehen, wenn Benutzer ihren PC während eines Scans abschalten, ein Host nach Verwendung eines Denial-of-Service-Plugins nicht mehr reagiert oder ein Sicherheitsmechanismus (z. B. ein IDS) die Datenübertragung an den Server gesperrt hat. Würde der Scan solcher Computer fortgesetzt, so würde unnötiger Datenverkehr im Netzwerk übertragen, und der Scan würde verzögert.
Avoid Sequential Scans (Fortlaufende Scans vermeiden)	Standardmäßig scannt Nessus eine Liste mit IP-Adressen in fortlaufender Reihenfolge. Wenn diese Option jedoch aktiviert ist, scannt Nessus die Liste in zufälliger Reihenfolge. Dies ist normalerweise nützlich, um den an ein bestimmtes Subnetz gerichteten Datenverkehr besser zu verteilen, wenn der Scan umfangreich ist.

Copyright © 2002-2011 Tenable Network Security, Inc.

Consider Unscanned Ports as Closed (Nicht gescannte Ports als geschlossen betrachten)	Wenn ein Port mit einem ausgewählten Portscanner nicht gescannt wird (weil er beispielsweise außerhalb des angegebenen Bereichs liegt), wird er von Nessus als geschlossen betrachtet.
Designate Hosts by their DNS Name (DNS-Namen für Hosts)	Wenn Sie diese Option auswählen, wird statt der IP-Adresse der Hostname in der Berichtsausgabe verwendet.

Im Bereich „**Network**" finden Sie Optionen, mit denen sich die Steuerung des Scans in Bezug auf das zu scannende Zielnetzwerk optimieren lässt:

Option	Beschreibung
Reduce Parallel Connections on Congestion (Parallele Verbindungen bei Überlast verringern)	Bei Aktivierung dieser Option kann Nessus erkennen, wenn zu viele Pakete versendet werden und die maximale Kapazität der Netzwerkverbindung in Kürze erreicht ist. In diesem Fall drosselt Nessus die Scanrate, um die Überlastung zu mindern. Nach Minderung der Überlastung versucht Nessus automatisch, die verfügbare Kapazität der Netzwerkverbindung wieder optimal zu nutzen.
Use Kernel Congestion Detection (Kernel-Überlastungserkennung verwenden, nur Linux)	Befähigt Nessus die CPU und andere interne Vorgänge auf Überlastung zu überwachen und die Verarbeitungsgeschwindigkeit bei Bedarf zu drosseln. Nessus wird immer versuchen, möglichst alle verfügbaren Ressourcen zu verwenden. Diese Funktionalität ist nur für Nessus-Scanner verfügbar, die auf einem Linux-System installiert sind.

Im Bereich „**Port Scanners**" („Portscanner") legen Sie fest, welche Methoden für das Scannen von Ports aktiviert werden sollen:

Option	Beschreibung
TCP Scan	Verwendet den integrierten TCP-Scanner von Nessus zur Ermittlung offener TCP-Ports auf den Zielsystemen. Dieser Scanner ist optimiert und verfügt über Selbstoptimierungsfunktionen. Auf einigen Plattformen (z. B. Windows und Mac OS X) startet Nessus stattdessen den SYN-Scanner, wenn durch den Einsatz des TCP-Scanners erhebliche Leistungseinbußen beim Betriebssystem zu erwarten sind.
UDP Scan	Verwendet den integrierten UDP-Scanner von Nessus zur Ermittlung offener UDP-Ports auf den Zielsystemen.

Copyright © 2002-2011 Tenable Network Security, Inc.

	UDP ist ein „zustandsloses" Protokoll, d. h. die Kommunikation erfolgt nicht über Handshake-Dialoge. Die UDP-basierte Kommunikation ist nicht immer zuverlässig und aufgrund der Eigenschaften von UDP-Diensten und –Auslesegeräten auch nicht immer remote erkennbar.
SYN Scan	Verwendet den integrierten SYN-Scanner von Nessus zur Ermittlung offener TCP-Ports auf den Zielsystemen. SYN-Scans sind ein beliebter Ansatz zur Durchführung von Portscans und gelten im Vergleich zu TCP-Scans allgemein als weniger aggressiv. Der Scanner sendet ein SYN-Paket an diesen Port, wartet auf die SYN-ACK-Antwort und bestimmt den Portstatus anhand der Antwort (bzw. anhand des Ausbleibens der Antwort).
SNMP Scan	Hiermit wird Nessus angewiesen, Ziele auf das Vorhandensein eines SNMP-Dienstes zu prüfen. Nessus versucht während eines SNMP-Scans, relevante Einstellungen zu erschließen. Wenn die Einstellungen durch den Benutzer unter „Preferences" angegeben wurden, kann Nessus den Remotehost besser testen und ausführlichere Auditresultate generieren. Beispielsweise gibt es eine ganze Reihe von Tests für Cisco-Router, mit denen durch Verarbeitung des zurückerhaltenen SNMP-Strings die vorhandenen Sicherheitslücken ermittelt werden. Diese Angaben sind für solche Audits erforderlich.
Netstat SSH Scan	Diese Option nutzt **`netstat`** zur Überprüfung offener Ports auf dem lokalen Computer. Hierzu wird auf den Befehl **`netstat`** zurückgegriffen, der über eine SSH-Verbindung mit dem Ziel verfügbar ist. Der Scan ist in erster Linie für Systeme auf UNIX-Basis gedacht und erfordert Anmeldedaten zur Authentifizierung.
Netstat WMI Scan	Diese Option nutzt **`netstat`** zur Überprüfung offener Ports auf dem lokalen Computer. Hierzu wird auf den Befehl **`netstat`** zurückgegriffen, der über eine WMI-Verbindung mit dem Ziel verfügbar ist. Der Scan ist in erster Linie für Windows-Systeme gedacht und erfordert Anmeldedaten zur Authentifizierung. Ein Scan auf WMI-Basis ermittelt mithilfe von **`netstat`** offene Ports, d. h. angegebene Portbereiche werden ignoriert. Wenn ein Port-Enumerator (Netstat oder SNMP) erfolgreich ist, umfasst der Portbereich nachfolgend alle Ports (Einstellung „all").
Ping Host (Pingbefehl an Host senden)	Diese Option ermöglicht das Senden von Pingbefehlen an Remotehosts über mehrere Ports, um festzustellen, ob sie

Copyright © 2002-2011 Tenable Network Security, Inc.

	online sind.

Über den Bereich „**Port Scan Options**“ („Optionen für Portscans“) wird ein bestimmter Portbereich als Zielbereich festgelegt. Die folgenden Werte sind für die Option „Port Scan Range“ („Portscanbereich“) zulässig:

Wert	Beschreibung
default (Standard)	Wenn das Schlüsselwort „default“ angegeben wird, scannt Nessus ca. 4.790 häufig verwendete Ports. Diese Liste der Ports kann der Datei **`nessus-services`** entnommen werden.
„all“ (Alle)	Wenn das Schlüsselwort „all“ angegeben wird, scannt Nessus alle 65.535 Ports.
Custom List (Benutzerdefinierte Liste)	Ein benutzerdefinierter Portbereich kann mithilfe einer Liste kommagetrennter Ports oder Portbereiche festgelegt werden. Beispielsweise sind Angaben wie „21,23,25,80,110“ oder „1-1024,8080,9000-9200“ zulässig. Wenn Sie „1-65535“ festlegen, werden alle Ports gescannt.

Der für einen Portscan angegebene Bereich ist gleichermaßen für TCP- und UDP-Scans gültig.

Im Bereich „**Performance**“ sind zwei Optionen vorhanden, mit denen die Anzahl der zu startenden Scans gesteuert wird. Diese Optionen sind möglicherweise bei der Konfiguration eines Scans am wichtigsten, denn sie haben die stärksten Auswirkungen auf Scandauer und Netzwerkaktivitäten.

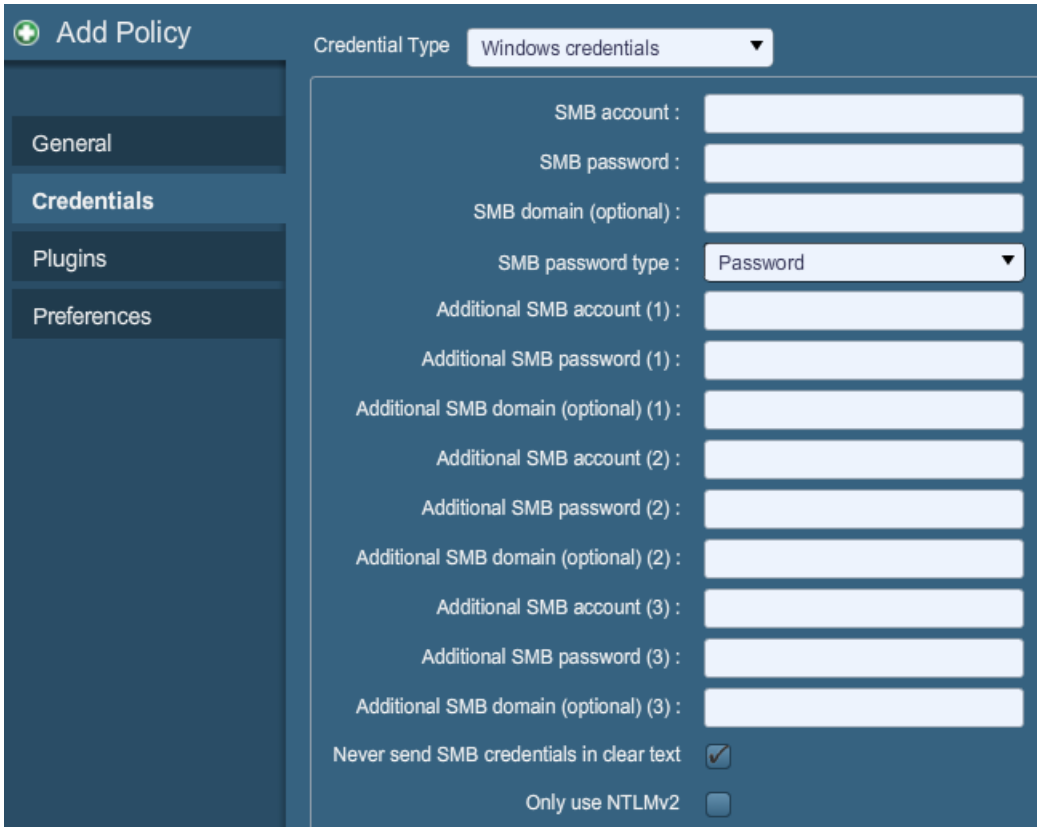
Option	Beschreibung
Max Checks Per Host (Tests je Host maximal)	Mit dieser Einstellung wird die Anzahl der Tests begrenzt, die ein Nessus-Scanner gleichzeitig für einen einzelnen Host ausführt.
Max Hosts Per Scan (Hosts je Scan maximal)	Mit dieser Einstellung wird die Anzahl der Hosts begrenzt, die von einem Nessus-Scanner gleichzeitig gescannt werden.
Network Receive Timeout (Timeout für Netzwerkdatenempfang, in Sekunden)	Der Standardwert liegt bei fünf Sekunden. Es handelt sich um die Zeit, für die Nessus auf eine Antwort von einem Host wartet (sofern durch ein Plugin nichts anderes festgelegt ist). Wenn Sie über eine langsame Verbindung scannen, sollten Sie hier einen höheren Wert eingeben.
Max Simultaneous TCP Sessions Per Host (Gleichzeitige Anzahl TCP-Sitzungen je Host	Durch diese Einstellung kann die Anzahl gleichzeitig laufender TCP-Sitzungen für einen einzelnen Host beschränkt werden.

Copyright © 2002-2011 Tenable Network Security, Inc.

maximal)	
Max Simultaneous TCP Sessions Per Scan (Gleichzeitige Anzahl TCP-Sitzungen je Scan maximal)	Durch diese Einstellung kann die Anzahl gleichzeitig laufender TCP-Sitzungen für den gesamten Scan beschränkt werden (die Anzahl der gescannten Hosts spielt hierbei keine Rolle). Bei Nessus-Scannern, die unter Windows XP, Vista oder 7 installiert sind, darf dieser Wert höchstens „19" betragen, da andernfalls keine korrekten Resultate zu erzielen sind.

Credentials

Auf der nachfolgend abgebildeten Registerkarte Credentials können Sie die Verwendung von Authentifizierungsdaten für Scanvorgänge durch den Nessus-Scanner konfigurieren. Nach der Konfiguration dieser Informationen kann Nessus eine größere Zahl von Tests ausführen und gelangt so zu genaueren Ergebnissen.



Im Dropdownmenü „**Windows credentials**" („Windows-Anmeldedaten") sind Einstellungen enthalten, um Nessus Informationen wie den Namen, das Kennwort und den Domänennamen für das SMB-Konto zu übermitteln. SMB (Server Message Block) ist ein Dateifreigabeprotokoll, mit dem Computer Daten im gesamten Netzwerk transparent verwenden können. Mithilfe dieser Angaben kann Nessus lokale Daten über einen Windows-Remotehost suchen. Beispielsweise kann Nessus

Copyright © 2002-2011 Tenable Network Security, Inc.

unter Verwendung der Authentifizierungsdaten feststellen, ob wichtige Sicherheitspatches bereits aufgespielt wurden. Die Standardwerte der anderen SMB-Parameter müssen nicht geändert werden.

Wenn ein SMB-Wartungskonto mit eingeschränkten Administratorrechten erstellt wird, kann Nessus auch mehrere Domänen einfach und sicher scannen.

Tenable empfiehlt Netzwerkadministratoren die Erstellung bestimmter Domänenkonten, um Tests zu vereinfachen. Nessus umfasst eine Vielzahl von Sicherheitstests für Windows NT, 2000, Server 2003, XP, Vista, Windows 7 und Windows 2008, die genauer arbeiten, wenn ein Domänenkonto angegeben wird. Allerdings versucht Nessus in den meisten Fällen, verschiedene Tests auch ohne Kontenangabe auszuführen.

Der Windows-Dienst „Remote-Registrierung" ermöglicht Remotecomputern mit entsprechenden Anmeldedaten den Zugriff auf die Registrierung des überprüften Computers. Wird der Dienst nicht ausgeführt, dann ist das Auslesen von Schlüsseln und Werten aus der Registrierung auch bei Angabe gültiger Authentifizierungsdaten nicht möglich. Weitere Informationen entnehmen Sie dem Tenable-Blogbeitrag „Dynamic Remote Registry Auditing - Now you see it, now you don't!".

Nach der Auswahl von „**SSH settings**" („SSH-Einstellungen") aus dem Dropdownmenü und der Eingabe von Anmeldedaten können UNIX-Systeme gescannt werden. Diese Anmeldedaten werden verwendet, um für Patchaudits oder Compliancetests lokale Informationen von UNIX-Remotesystemen abzurufen. Es sind Felder für die Eingabe des SSH-Benutzernamens für das Konto vorhanden, unter dem die Tests auf dem UNIX-Zielsystem ausgeführt werden, sowie für das SSH-Kennwort oder das SSH-Schlüsselpaar (öffentlicher und geheimer Schlüssel). In ein weiteres Feld können Sie ggf. die Passphrase für den SSH-Schlüssel eingeben.

Nessus 4 unterstützt die Verschlüsselungsalgorithmen **`blowfish-cbc`**, **`aes-cbc`** und **`aes-ctr`**.

Die wirksamsten authentifizierten Scans sind solche, bei denen das angegebene Konto über Root-Berechtigungen verfügt. Da zahlreiche Sites eine Remoteanmeldung als Root nicht zulassen, können Nessus-Benutzer „**`su`**" oder „**`sudo`**" mit einem separaten Kennwort für ein Konto aufrufen, für das „**`su`**"- oder „**`sudo`**"-Berechtigungen konfiguriert wurden.

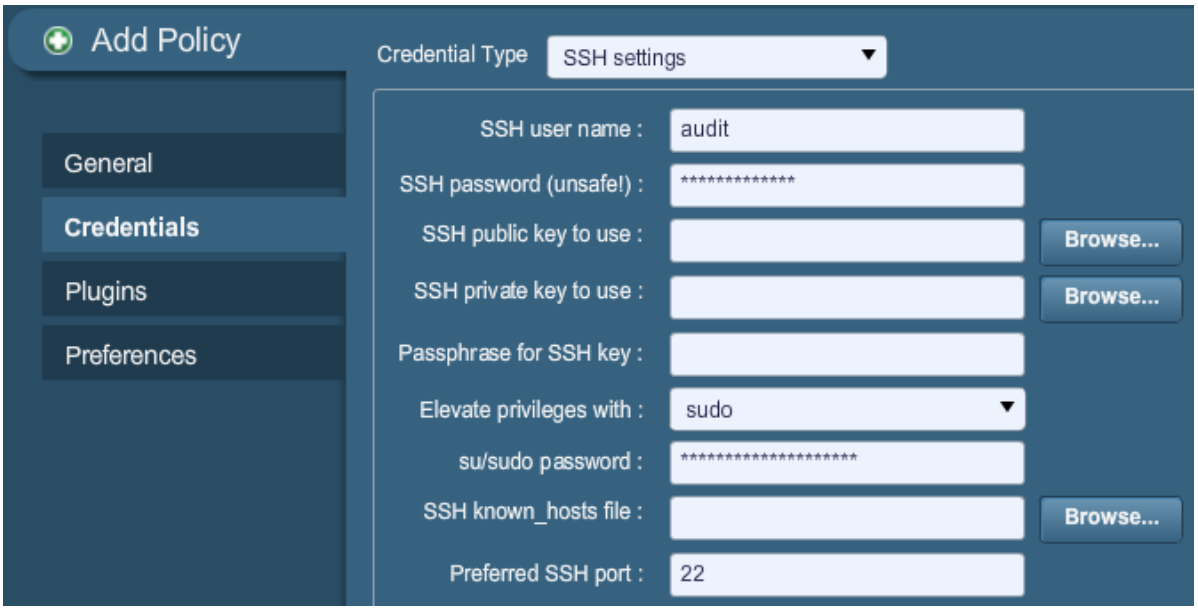
Nessus kann zur Authentifizierung bei einem Remoteserver einen Zugriff auf SSH-Basis verwenden. Wenn die SSH-Datei „ known_hosts " vorhanden und als Teil der Scanrichtlinie angegeben ist, wird Nessus sich, sofern möglich, nur bei den in dieser Datei genannten Hosts anmelden. Schließlich kann unter „Preferred SSH port" noch der bevorzugte SSH-Port festgelegt werden, falls Nessus die Verbindung mit SSH über einen anderen als den Standardport 22 herstellen soll.

Nessus verschlüsselt alle in den Richtlinien gespeicherten Kennwörter. Allerdings sehen die Best Practices vor, zur Authentifizierung SSH-Schlüssel anstelle von SSH-Kennwörtern zu verwenden. Auf diese Weise soll sichergestellt werden, dass derselbe Benutzername und dasselbe Kennwort, die Sie für Audits Ihrer bekannten SSH-Server verwenden, nicht zur Anmeldung auf einem System verwendet wird, das sich nicht unter ihrer Kontrolle befindet. Aufgrund dessen wird zur Verwendung von SSH-Kennwörtern nur dann geraten, wenn es absolut unabdingbar ist.

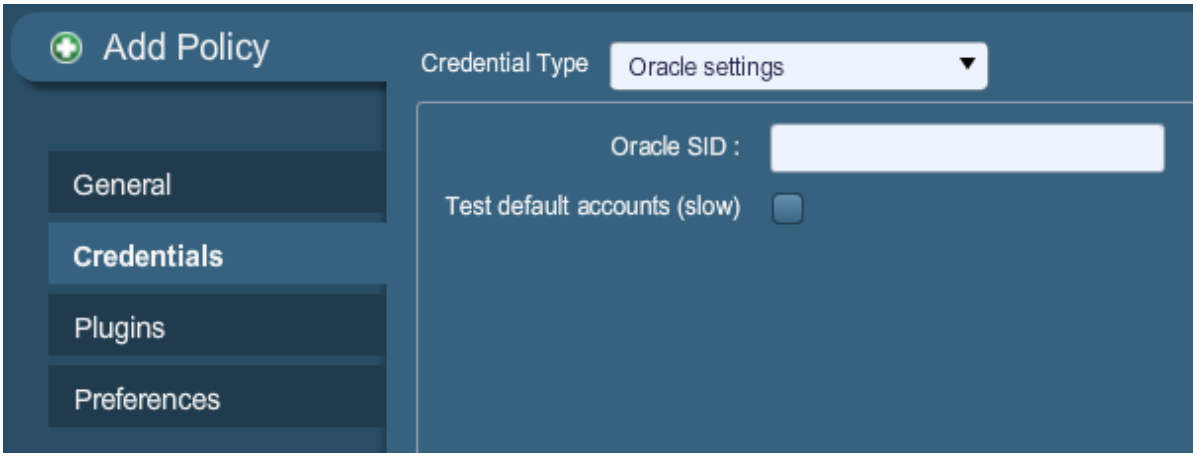
Copyright © 2002-2011 Tenable Network Security, Inc.

Nessus unterstützt auch die Option „su+sudo". Diese kann verwendet werden, falls ein System keine Berechtigungen für die Remoteanmeldung berechtigter Konten gestattet.

Es folgt eine Bildschirmabbildung für die Verwendung von „**`sudo`**" zum Hochstufen von Berechtigungen für einen Scan. In diesem Beispiel heißt das Benutzerkonto „audit" und wurde der Datei **`/etc/sudoers`** auf dem zu scannenden System hinzugefügt. Angegeben wird das Kennwort für das Konto „audit", nicht das Root-Kennwort:



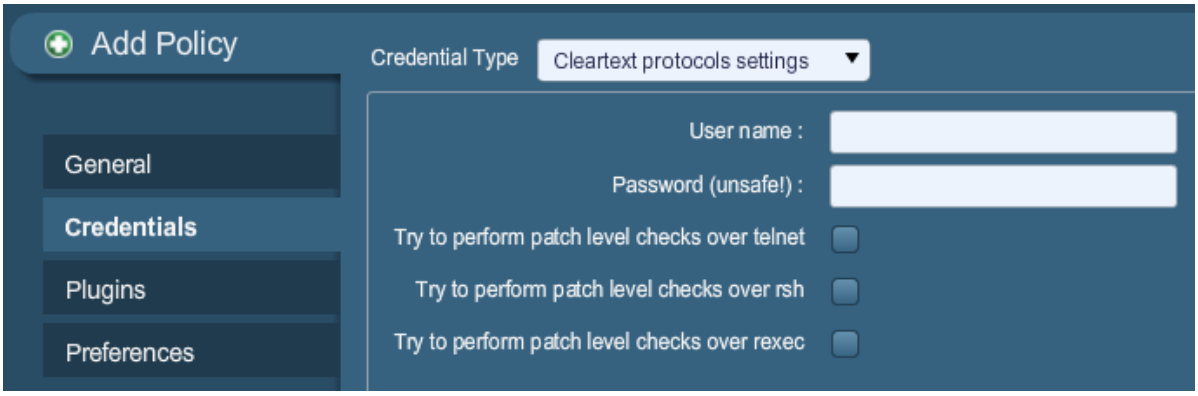
Die Registerkarte Credentials stellt außerdem im Dropdownmenü die Option „**Oracle settings**" („Oracle-Einstellungen") zur Einstellung der Oracle-SID (Parameter „ Oracle SID") bereit sowie eine Option zum Test auf das Vorhandensein bekannter Konten in der Oracle-Software:



Mit „**Kerberos configuration**" („Kerberos-Konfiguration") können Sie Anmeldedaten unter Verwendung von Kerberos-Schlüsseln von einem Remotesystem aus angeben:

Copyright © 2002-2011 Tenable Network Security, Inc.

Schließlich kann, wenn eine sichere Methode zur Durchführung authentifizierter Tests nicht verfügbar ist, der Versuch erzwungen werden, Nessus-Tests über unsichere Protokolle durchzuführen. Hierzu muss das Element „**Cleartext protocol settings**" („Einstellungen für unverschlüsselte Protokolle") im Dropdownmenü konfiguriert werden. Unterstützt werden für diese Option die unverschlüsselten Protokolle **telnet**, **rsh** und **rexec**.



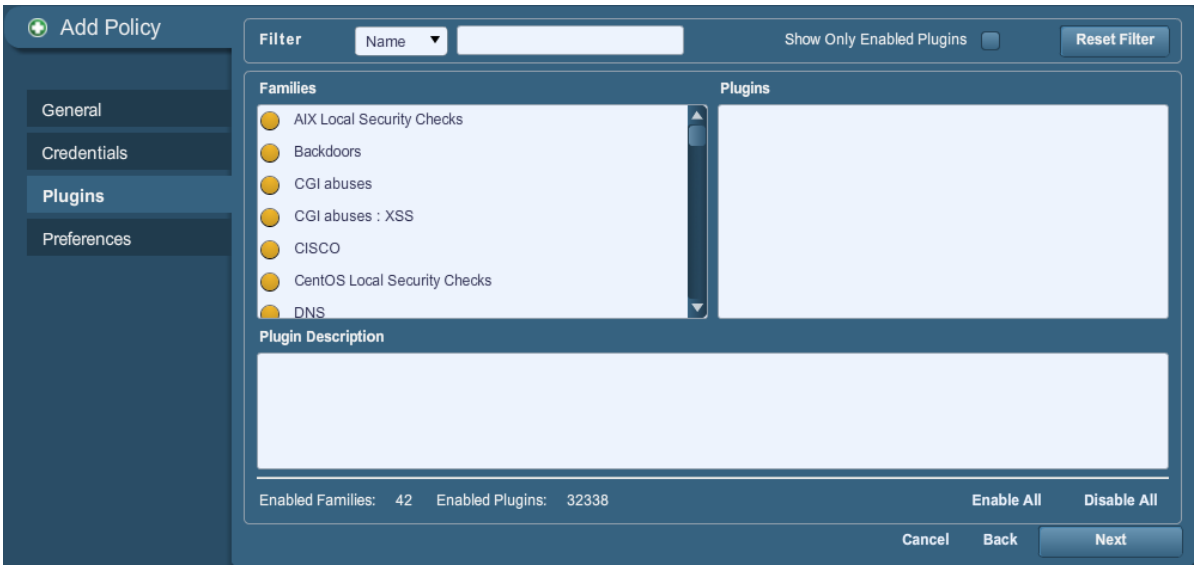
Standardmäßig sind alle Kennwörter (und auch die Richtlinie selbst) verschlüsselt. Wird die Richtlinie in einer `.nessus`-Datei gespeichert und diese Datei nachfolgend auf eine andere Nessus-Installation kopiert, dann sind die Kennwörter für den zweiten Nessus-Scanner unzugänglich, da er sie nicht entschlüsseln kann.

Von der Verwendung unverschlüsselter Authentifizierungsdaten wird **dringend** abgeraten! Werden die Anmeldedaten remote (z. B. bei einem Nessus-Scan) übermittelt, dann können sie von jeder Person abgefangen werden, die Zugriff auf das Netzwerk hat. Deswegen sollten Sie, sofern dies irgendwie möglich ist, Mechanismen zur verschlüsselten Authentifizierung verwenden.

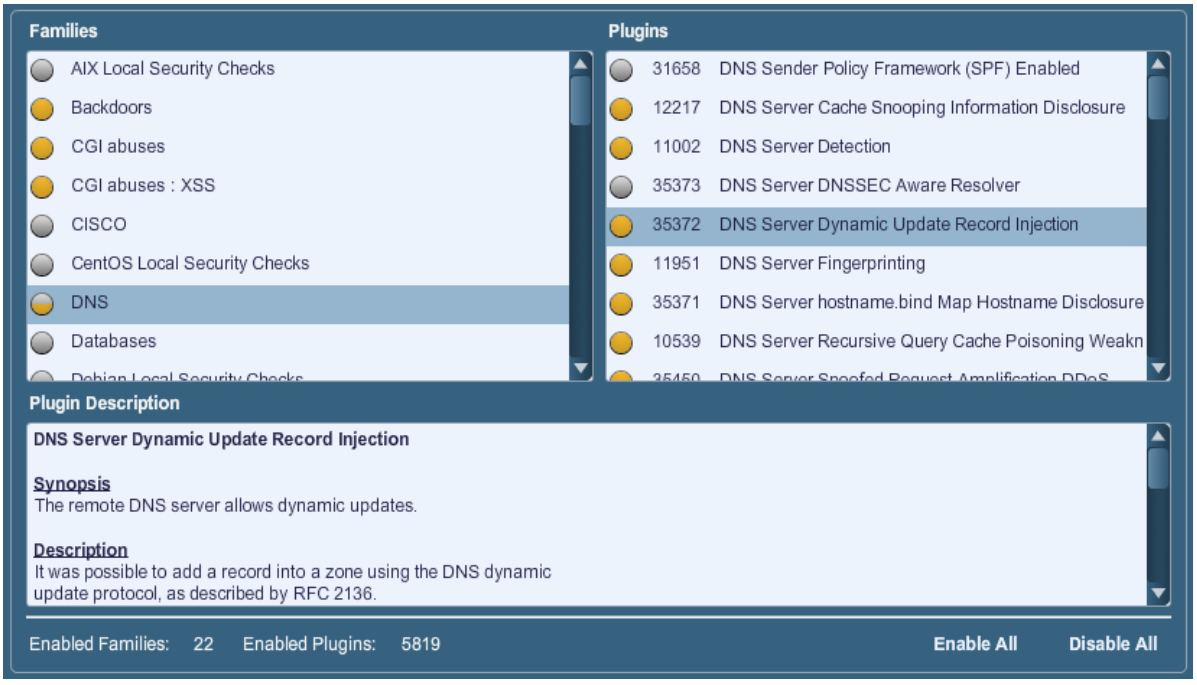
Plugins

Die Registerkarte „Plugin Selection" („Plugin-Auswahl") ermöglicht die Auswahl bestimmter Sicherheitstests durch Plugin-Familien wie auch einzelne Tests.

Copyright © 2002-2011 Tenable Network Security, Inc.



Durch Anklicken des gelben Kreises neben einer Plugin-Familie können Sie die gesamte Familie aktivieren oder deaktivieren. Bei Auswahl einer Familie wird die Liste der zugehörigen Plugins in der oberen rechten Ecke angezeigt. Einzelne Plugins können separat aktiviert oder deaktiviert werden, um die Scanrichtlinien exakt für den eigenen Bedarf maßzuschneidern. Während Sie die Einstellungen vornehmen, werden die Gesamtzahl der ausgewählten Familien und Plugins unten im Fenster angezeigt. Wenn der Kreis neben einer Plugin-Familie zur Hälfte grau und zur anderen Hälfte gelb ist, weist dies darauf hin, dass einige, aber nicht alle Plugins aktiviert sind.

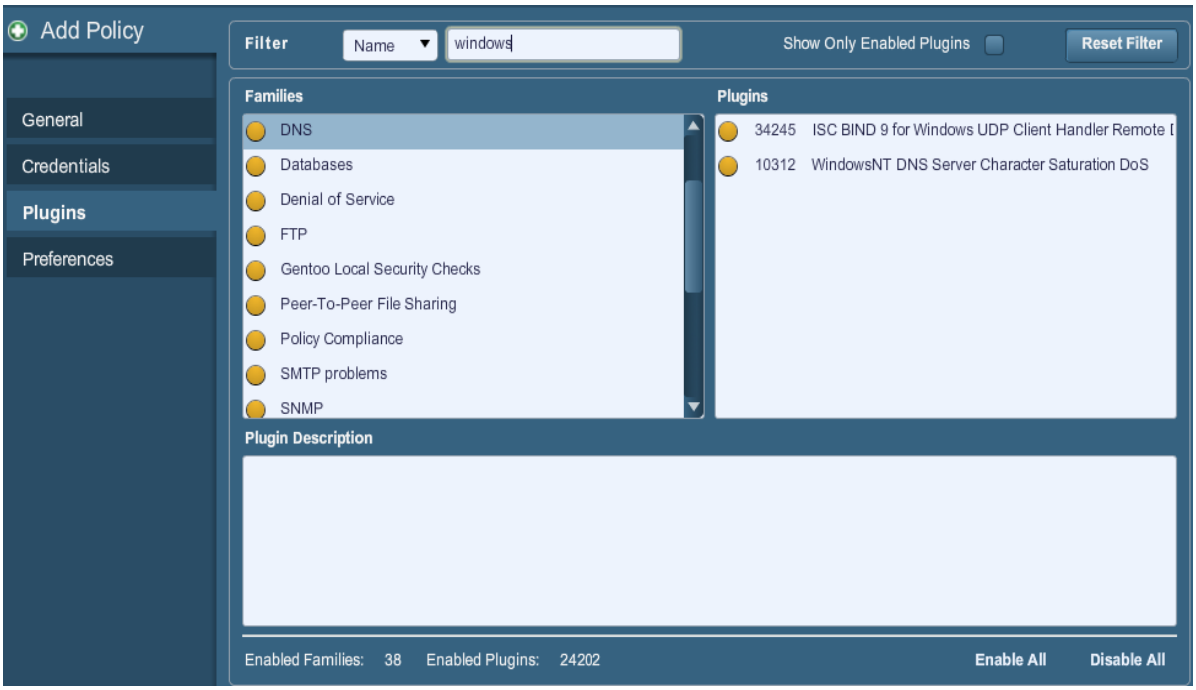

Families
Plugins
AIX Local Security Checks
Backdoors
CGI abuses
CGI abuses : XSS
CISCO
CentOS Local Security Checks
DNS
Databases
31658 DNS Sender Policy Framework (SPF) Enabled
12217 DNS Server Cache Snooping Information Disclosure
11002 DNS Server Detection
35373 DNS Server DNSSEC Aware Resolver
35372 DNS Server Dynamic Update Record Injection
11951 DNS Server Fingerprinting
35371 DNS Server hostname.bind Map Hostname Disclosure
10539 DNS Server Recursive Query Cache Poisoning Weakn
Plugin Description
DNS Server Dynamic Update Record Injection
Synopsis
The remote DNS server allows dynamic updates.
Description
It was possible to add a record into a zone using the DNS dynamic update protocol, as described by RFC 2136.
Enabled Families: 22
Enabled Plugins: 5819
Enable All
Disable All

Bei Auswahl eines Plugins wird dessen Ausgabe so angezeigt, wie sie später in einem Bericht enthalten sein wird. Die Zusammenfassung und die Beschreibung enthalten weitere Details zur untersuchten Sicherheitslücke. Wenn Sie im Bereich „Plugin Description" („Plugin-Beschreibung") nach unten blättern, erscheinen auch Hinweise zur Behebung, ggf.

Copyright © 2002-2011 Tenable Network Security, Inc.

weitere Verweise und die CVSSv2-Bewertung (mit dieser wird eine allgemeine Risikobewertung angegeben).

Ganz oben auf der Registerkarte für die Plugin-Familien können Sie nach einem bestimmten Plugin suchen. Hierzu geben Sie wahlweise den Namen oder die ID an. Im Feld „**Filter**" können Sie zu suchenden Text eingeben. Danach betätigen Sie die Eingabetaste:



Wenn eine Richtlinie erstellt und gespeichert wird, sind in ihr alle Plugins vermerkt, die ursprünglich ausgewählt wurden. Wenn neue Plugins über ein Plugin-Feedupdate empfangen werden, werden diese automatisch aktiviert, sofern die zugehörige Familie in der Richtlinie bereits aktiviert ist. Wurde die Familie vollständig oder teilweise deaktiviert, dann werden auch neue Plugins dieser Familie automatisch deaktiviert.

Die Familie „Denial of Service" enthält einige Plugins, die in einem Firmennetzwerk Ausfälle verursachen könnten, wenn die Option „Safe Checks" deaktiviert ist; auf der anderen Seite enthält sie auch einige nützliche Tests, die keinen Schaden anrichten können. Sie können die Familie „Denial of Service" in Verbindung mit der aktivierten Option „Safe Checks" verwenden, um sicherzustellen, dass potenziell gefährliche Plugins nicht ausgeführt werden. Wir empfehlen allerdings, die Familie „Denial of Service" in einem Produktionsnetzwerk nicht einzusetzen.

Unter dem Fenster, das die Plugins auflistet, befinden sich zwei Optionen, die Ihnen bei der Auswahl der Plugins behilflich sein werden.

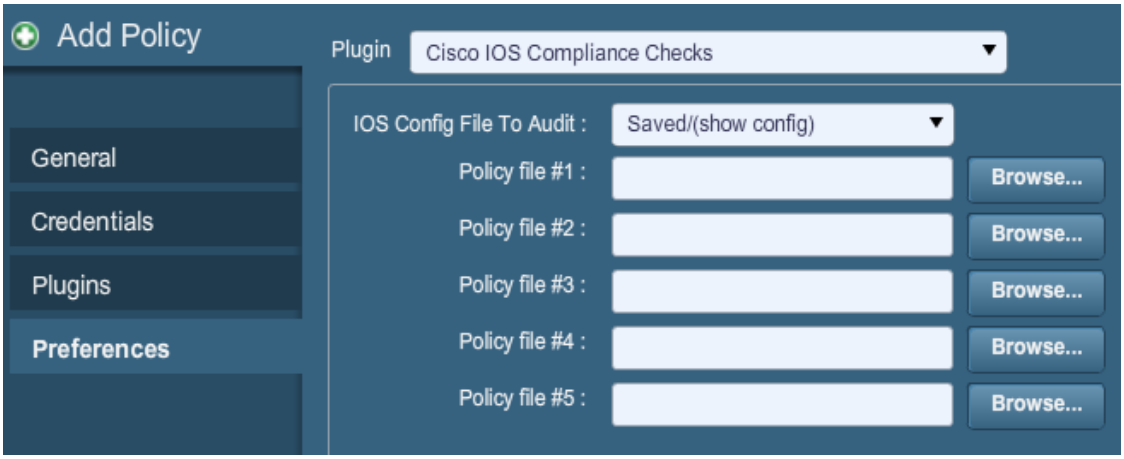
Option	Beschreibung
Enable all (Alle aktivieren)	Hiermit werden alle Plugins und ihre Familien ausgewählt und aktiviert. Es handelt sich hierbei um eine einfache

Copyright © 2002-2011 Tenable Network Security, Inc.

	Möglichkeit, alle Plugins zu reaktivieren, wenn Sie zuvor eine Richtlinie erstellt haben, in der einige Familien oder Plugins deaktiviert wurden. Beachten Sie, dass für einige Plugins weitere Optionen konfiguriert werden müssen.
Disable all (Alle deaktivieren)	Hiermit werden alle Plugins und ihre Familien abgewählt und deaktiviert. Wenn Sie einen Scan ausführen, bei dem alle Plugins deaktiviert sind, werden keine Ergebnisse generiert.

Preferences

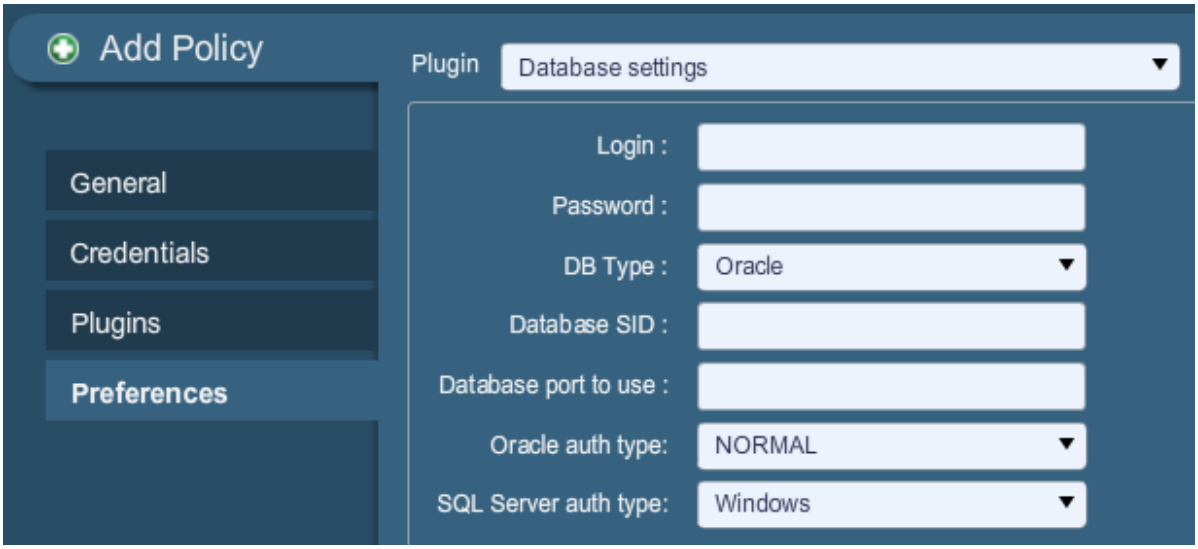
Die Registerkarte „**Preferences**" („Voreinstellungen") enthält Optionen für eine fein abgestufte Steuerung der Scaneinstellungen. Bei Auswahl eines Elements aus dem Dropdownmenü werden weitere Konfigurationselemente für die ausgewählte Kategorie angezeigt. Beachten Sie, dass die Liste der Konfigurationsoptionen dynamisch ist, d. h. sie hängt vom Plugin-Feed, von den Auditrichtlinien und weiteren Funktionen ab, auf die der verbundene Nessus-Scanner zugreifen kann. Bei einem Scanner mit einem ProfessionalFeed stehen unter Umständen mehr fortgeschrittene Konfigurationsoptionen zur Verfügung als bei einem Scanner, für den der HomeFeed konfiguriert wurde. Außerdem kann sich diese Liste ändern, wenn Plugins hinzugefügt oder geändert werden.



Mit der Option „**Cisco IOS Compliance Checks**" („Cisco IOS-Compliancetests") können ProfessionalFeed-Kunden Richtliniendateien hochladen, anhand derer ermittelt wird, ob ein getestetes Gerät, das unter Cisco IOS läuft, die angeforderten Compliancestandards erfüllt. Bis zu fünf Richtlinien können gleichzeitig ausgewählt werden. Diese Richtlinien können für die gespeicherte Konfiguration (SaveConfig, **`show config`**), die laufende Konfiguration (RunningConfig, **`show running`**) oder die Startkonfiguration (StartConfig, **`show startup`**) ausgeführt werden.

Copyright © 2002-2011 Tenable Network Security, Inc.

Mit der Option „**Database Compliance Checks**" („Datenbank-Compliancetests") können ProfessionalFeed-Kunden Richtliniendateien hochladen, anhand derer ermittelt wird, ob eine getestete Datenbank die angeforderten Compliancestandards erfüllt. Bis zu fünf Richtlinien können gleichzeitig ausgewählt werden.



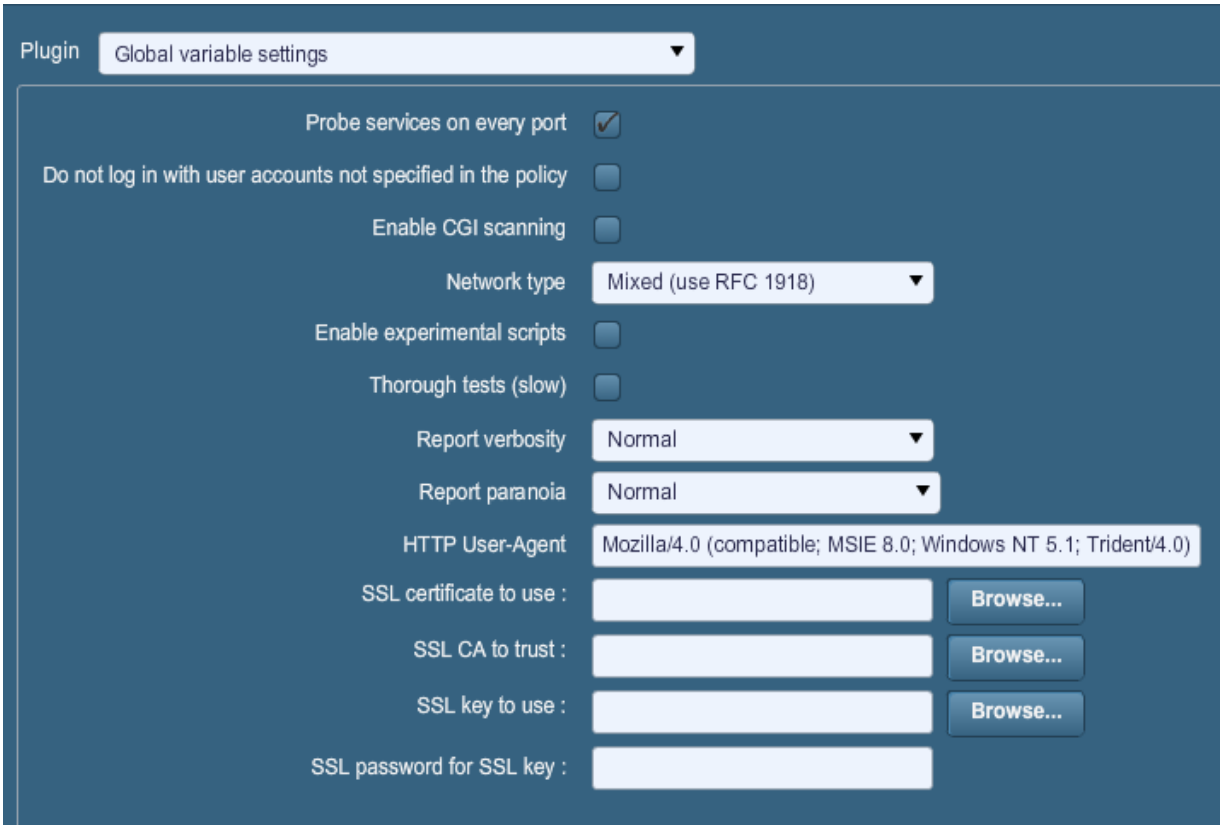
Mithilfe der Optionen unter „**Database settings**" („Datenbankeinstellungen") werden der Typ der zu testenden Datenbank, zugehörige Einstellungen und Anmeldedaten angegeben:

Option	Beschreibung
Login (Anmeldename)	Der Benutzername für die Datenbank.
Password (Kennwort)	Das Kennwort zum angegebenen Benutzernamen.
DB Type (Datenbanktyp)	Oracle, SQL Server, MySQL, DB2, Informix/DRDA und PostgreSQL werden unterstützt.
Database SID (System-ID der Datenbank)	System-ID der zu überwachenden Datenbank.

Copyright © 2002-2011 Tenable Network Security, Inc.

Database port to use (Zu verwendender Datenbankport)	Port, auf dem die Datenbank horcht.
Oracle auth type (Oracle-Authentifizierungstyp)	NORMAL, SYSOPER und SYSDBA werden unterstützt.
SQL Server auth type (SQL Server-Authentifizierungstyp)	Windows und SQL werden unterstützt.

Die Option „**Do not scan fragile devices**" („Unbelastbare Geräte nicht scannen") weist den Nessus-Scanner an, Drucker und Novell Netware-Hosts auch dann nicht zu scannen, wenn sie ausgewählt wurden. Da diese beiden Technologien recht anfällig für Denial-of-Service-Bedingungen sind, kann Nessus sie beim Scannen übergehen. Dies wird empfohlen, wenn Scans während der Geschäftszeit ausgeführt werden.



Die „**Global variable settings**" („Globale Variableneinstellungen") enthalten eine Vielzahl von Konfigurationsoptionen für den Nessus-Server.

Option	Beschreibung
Probe services on every port (Dienste auf jedem	Bei Auswahl dieser Option wird versucht, jedem offenen Port den Dienst zuzuordnen, der auf diesem Port ausgeführt

Copyright © 2002-2011 Tenable Network Security, Inc.

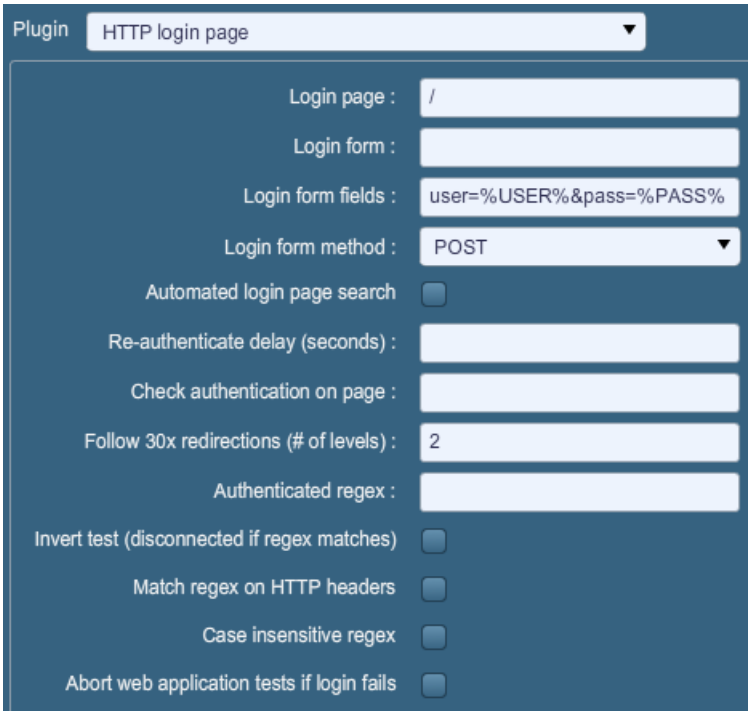
Port testen)	wird. Beachten Sie, dass es in seltenen Fällen zu Störungen einiger Dienste und zu nicht vorhersehbaren Nebeneffekten kommen kann.
Do not log in with user accounts not specified in the policy (Keine Anmeldung mit Benutzerkonten, die in der Richtlinie nicht angegeben sind)	Hiermit werden Kontensperrungen verhindert, wenn Ihre Kennwortrichtlinie vorsieht, dass Konten nach mehreren ungültigen Anmeldeversuchen gesperrt werden.
Enable CGI scanning (CGI-Scans aktivieren)	Hiermit werden CGI-Tests aktiviert. Durch Deaktivierung dieser Option wird ein Audit eines lokalen Netzwerks ganz erheblich beschleunigt.
Network type (Netzwerktyp)	Hier können Sie angeben, ob Sie öffentliche oder private IP-Adressen oder eine Kombination dieser beiden Typen verwenden. Wählen Sie „Mixed" („Gemischt") aus, wenn Sie RFC 1918-Adressen verwenden und mehrere Router in Ihrem Netzwerk einsetzen.
Enable experimental scripts (Experimentelle Skripts verwenden)	Gestattet die Verwendung von als experimentell betrachteten Plugins für den Scan. Lassen Sie diese Option deaktiviert, wenn Sie ein Produktionsnetzwerk scannen.
Thorough tests (slow) (Umfassende Tests, langsam)	Wenn Sie diese Option aktivieren, wird die Testleistung bestimmter Plugins erhöht. Wenn Sie beispielsweise SMB-Dateifreigaben überprüfen, kann das Plugin bei aktivierter Option eine Analysetiefe von drei Stufen (statt einer Stufe) verwenden. In bestimmten Fällen kann die Auswahl dieser Option sowohl die Analyse verlängern als auch das Datenaufkommen im Netzwerk erheblich erhöhen. Beachten Sie auch, dass umfassende Scans aggressiver vorgehen und Störungen im Netzwerk wahrscheinlicher sind; dafür sind die Auditergebnisse aussagekräftiger.
Report verbosity (Berichtsausführlichkeit)	Je höher der hier zugewiesene Wert, desto mehr oder weniger Informationen zu Plugin-Aktivitäten fließen in den Bericht.
Report paranoia (Maximale Sicherheit im Bericht)	In einigen Fällen kann von Nessus remote nicht bestimmt werden, ob tatsächlich ein Schwachpunkt vorliegt. Wenn Sie für diese Optionen die Einstellung „**Paranoid**" auswählen, wird in jedem Fall ein Schwachpunkt gemeldet, auch wenn ein Fehlalarm nicht ausgeschlossen werden kann. Umgekehrt führt die Einstellung „**Avoid false alarm**" („Fehlalarme vermeiden") dazu, dass Nessus einen Schwachpunkt nicht meldet, wenn nicht sicher ist, dass er vorhanden ist. Die Standardoption („**Normal**") stellt einen Kompromiss zwischen den vorgenannten beiden Einstellungen dar.
HTTP User-Agent	Hiermit wird angegeben, welchen Webbrowsertyp Nessus beim Scannen emuliert.

Copyright © 2002-2011 Tenable Network Security, Inc.

SSL certificate to use (Zu verwendendes SSL-Zertifikat)	Ermöglicht Nessus die Verwendung eines clientseitigen SSL-Zertifikat für die Kommunikation mit einem Remotehost.
SSL CA to trust (Vertrauenswürdige SSL-Zertifizierungsstelle)	Hier wird eine Zertifizierungsstelle (Certificate Authority, CA) angegeben, die Nessus als vertrauenswürdig einstuft.
SSL key to use (Zu verwendender SSL-Schlüssel)	Hiermit wird ein lokaler SSL-Schlüssel zur Verwendung für die Kommunikation mit dem Remotehost angegeben.
SSL password for SSL key (SSL-Kennwort für SSL-Schlüssel)	Hier geben Sie das Kennwort zur Verwaltung des angegebenen SSL-Schlüssels an.

Zur Ermöglichung von Webanwendungstests kann Nessus HTTP-Cookies aus einer anderen Software (z. B. Webbrowser, Webproxy usw.) importieren. Der Import wird mit den Einstellungen unter „**HTTP cookies import**" (HTTP-Cookieimport) gesteuert. Eine Cookiedatei kann hochgeladen werden, damit Nessus die Cookies für den Zugriff auf eine Webanwendung verwendet. Die Cookiedatei muss im Netscape-Format vorliegen.

Copyright © 2002-2011 Tenable Network Security, Inc.

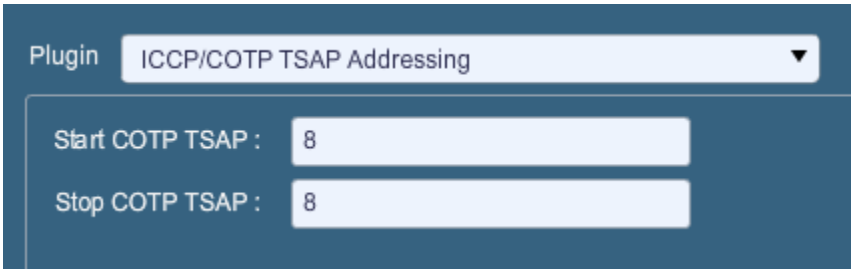


Mit den Einstellungen unter „**HTTP login page**" („HTTP-Anmeldeseite") können Sie festlegen, an welcher Stelle authentifizierte Tests einer benutzerdefinierten webbasierten Anwendung beginnen.

Option	Beschreibung
Login page (Anmeldeseite)	Dies ist die Basis-URL der Anmeldeseite der Anwendung.
Login form (Anmeldeformular)	Beispielsweise würde das Anmeldeformular für `<form method="POST" name="auth_form" action="/login.php">` den Wert „**`/login.php`**" haben.
Login form fields (Anmeldeformularfelder)	Geben Sie die Authentifizierungsparameter (z. B. `login=%USER%&password=%PASS%`) ein. Wenn die Schlüsselwörter %USER% und %PASS% verwendet werden, werden diese durch die Werte ersetzt, die im Dropdownmenü „Login configurations" („Anmeldekonfiguration") angegeben werden. Mithilfe dieses Feldes können, falls erforderlich, auch zwei Parameter angegeben werden (z. B. ein „Gruppenname" oder andere Angaben, die für den Authentifizierungsprozess erforderlich sind).
Login form method (Anmeldeformularmethode)	Geben Sie an, ob die Anmeldeaktion über eine GET- oder eine POST-Anforderung erfolgt.
Automated login page search (Automatische Suche der Anmeldeseite)	Hiermit wird Nessus angewiesen, nach einer Anmeldeseite zu suchen.

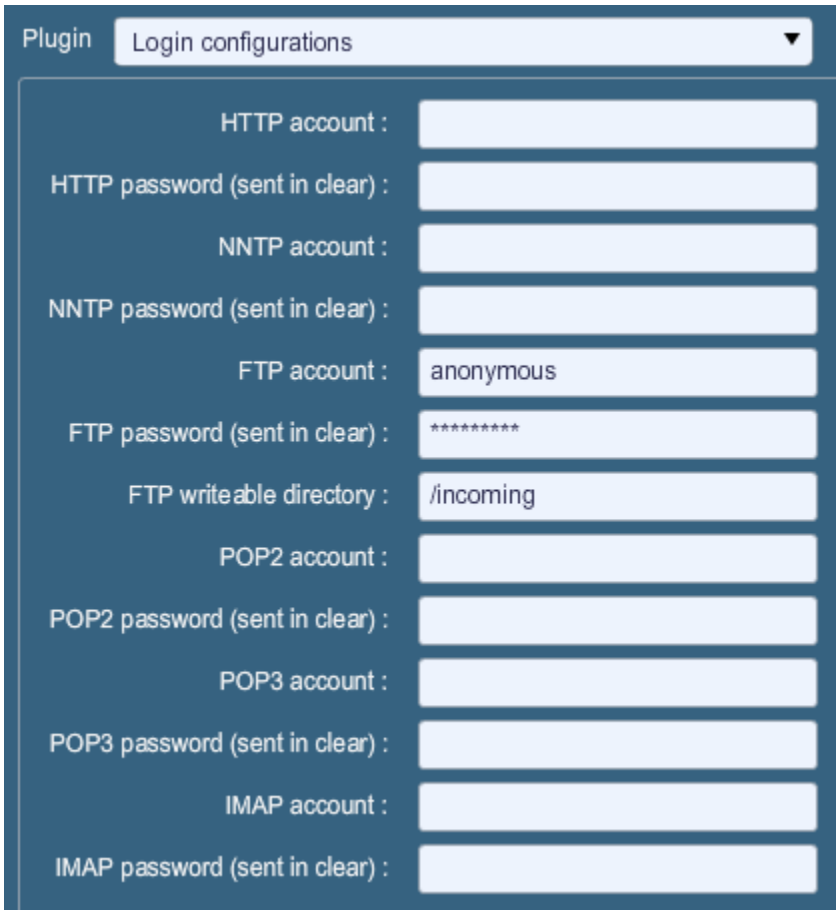
Copyright © 2002-2011 Tenable Network Security, Inc.

Re-authenticate delay (seconds) (Verzögerung für Neuauthentifizierung, in Sekunden)	Zeitliche Verzögerung bis zum nächsten Authentifizierungsversuch. Dieser Parameter ist nützlich, um das Auslösen von Schutzmechanismen gegen Brute-Force-Angriffe zu vermeiden.
Check authentication on page (Authentifizierung auf der Seite überprüfen)	Hier wird die URL einer geschützten Webseite angegeben, die eine Authentifizierung erfordert. Auf diese Weise kann Nessus den Authentifizierungsstatus einfacher feststellen.
Follow 30x redirections (# of levels) (30x-Umleitungen folgen, Anzahl der Ebenen)	Wenn ein 30x-Umleitungscode von einem Webserver empfangen wird, wird hier festgelegt, ob dieser Nessus an den angegebenen Link weiterleitet.
Authenticated regex (Authentifizierter regulärer Ausdruck)	Ein regulärer Ausdruck, nach dem auf der Anmeldeseite gesucht werden soll. Manchmal ist es zur Feststellung des Sitzungsstatus nicht ausreichend, einfach nur einen 200-Antwortcode zu erhalten. Nessus kann versuchen, einen Vergleich auf Vorhandensein eines angegebenen Strings wie beispielsweise „Authentication successful!" („Authentifizierung erfolgreich") durchzuführen.
Invert test (disconnected if regex matches) (Test umkehren (Trennung bei Übereinstimmung mit regulärem Ausdruck))	Ein regulärer Ausdruck, nach dem auf der Anmeldeseite gesucht wird. Wenn die Suche erfolgreich ist, wird Nessus mitgeteilt, dass die Authentifizierung fehlgeschlagen ist (Beispiel: „Authentication failed!")
Match regex on HTTP headers (HTTP-Header mit regulärem Ausdruck vergleichen)	Anstelle des Datenteils einer HTTP-Antwort kann Nessus auch die Header (Kopfdaten) der Antwort nach einem bestimmten regulären Ausdruck durchsuchen, um den Authentifizierungsstatus besser ermitteln zu können.
Case insensitive regex (Keine Unterscheidung der Groß-/Kleinschreibung bei regulären Ausdrücken)	Bei Suchvorgängen mit regulären Ausdrücken wird die Groß-/Kleinschreibung standardmäßig beachtet. Mit dieser Option können Sie Nessus anweisen, die Groß-/Kleinschreibung zu ignorieren.
Abort web application tests if login fails (Bei fehlgeschlagener Anmeldung Webanwendungstests abbrechen)	Wenn die angegebenen Anmeldedaten nicht funktionieren, bricht Nessus die benutzerdefinierten Webanwendungstests ab (nicht jedoch die CGI-Plugin-Familien).

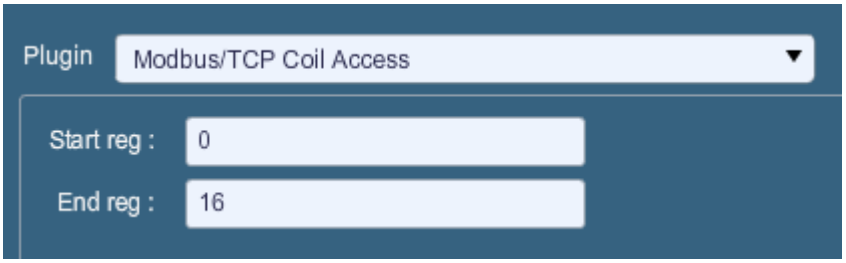


Copyright © 2002-2011 Tenable Network Security, Inc.

Das Menü „**ICCP/COTP TSAP Addressing**“ („ICCP/COTP-TSAP-Adressierung“) dient vor allem der Konfiguration von SCADA-Tests. Es bestimmt durch Ausprobieren möglicher Werte einen COTP-TSAP-Wert (Connection Oriented Transport Protocol/Transport Service Access Points) auf einem ICCP-Server. Die Start- und Stoppwerte sind standardmäßig auf „8“ festgelegt.



Mit „**Login configurations**“ („Anmeldekonfigurationen“) wird dem Nessus-Scanner die Verwendung von Anmeldedaten beim Testen von HTTP, NNTP, FTP, POP2, POP3 oder IMAP ermöglicht. Wenn Anmeldedaten angegeben werden, kann Nessus ausführlichere Tests zur Erkennung von Sicherheitslücken ausführen. Hier angegebene HTTP-Anmeldedaten werden nur für die Basis- und die Digest-Authentifizierung verwendet. Verwenden Sie zur Konfiguration der Anmeldedaten für eine angepasste Webanwendung das Pulldownmenü „HTTP login page“ („HTTP-Anmeldeseite“).



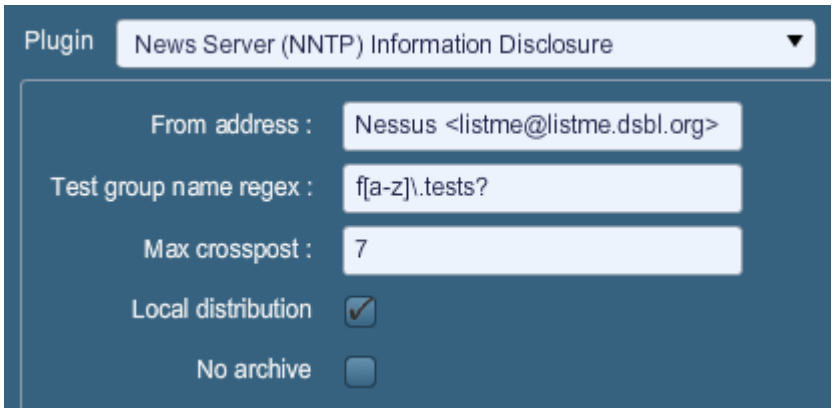
Die Optionen unter „**Modbus/TCP Coil Access**“ („Modbus-/TCP-Coil-Zugriff“) stehen nur ProfessionalFeed-Benutzern zur Verfügung. Dieses Dropdownmenü wird durch die SCADA-Plugins, die Bestandteil des ProfessionalFeed sind, dynamisch generiert. Modbus verwendet

Copyright © 2002-2011 Tenable Network Security, Inc.

den Funktionscode „1" zum Auslesen der „Coils" auf einem Modbus-Slave. Coils stellen binäre Ausgabeeinstellungen dar und sind gewöhnlich Auslösern zugeordnet. Beim Lesen von Coils kann ein Angreifer möglicherweise ein Systemprofil erstellen und Registerbereiche erkennen, die er dann über einen Write-Coil-Befehl ändern kann. Die Standardwerte sind „0" für das Start-Register und „16" für das End-Register.

Mit den Optionen „**Nessus SYN scanner**" und „**Nessus TCP scanner**" können Sie die Erkennung einer Firewall durch die nativen SYN- bzw. TCP-Scanner verbessern.

Wert	Beschreibung
Automatic (normal) (Automatisch (normal))	Durch Einstellung dieser Option kann einfacher erkannt werden, ob sich eine Firewall zwischen dem Scanner und dem Zielsystem befindet (**Standard**).
Disabled (softer) (Inaktiv (weniger aggressiv))	Hierdurch wird die Funktion **Firewall detection** („Firewallerkennung") deaktiviert.
Do not detect RST rate limitation (soft) (RST-Ratenbeschränkung nicht erkennen (weniger aggressiv))	Hiermit wird die Möglichkeit deaktiviert, festzustellen, wie häufig Resets festgelegt werden und ob auf einem nachgeschalteten Netzwerkgerät eine Beschränkung konfiguriert ist.
Ignore closed ports (aggressive) (Geschlossene Ports ignorieren (aggressiv))	Hierbei wird versucht, Plugins auch dann auszuführen, wenn der Port geschlossen zu sein scheint. Es wird nicht empfohlen, diese Option in einem Produktionsnetzwerk einzusetzen.



Mithilfe der Option „**News Server (NNTP) Information Disclosure**" („Offenlegung von Newsserver-(NNTP-)Daten") kann bestimmt werden, ob vorhandene Newsserver zur Weiterleitung von Spam verwendet werden. Nessus versucht, einen Newsbeitrag an einen oder mehrere NNTP-Server (Network News Transport Protocol) zu schicken, und kann dann überprüfen, ob es möglich ist, diesen Beitrag auch an nachgeschaltete Newsserver zu schicken.

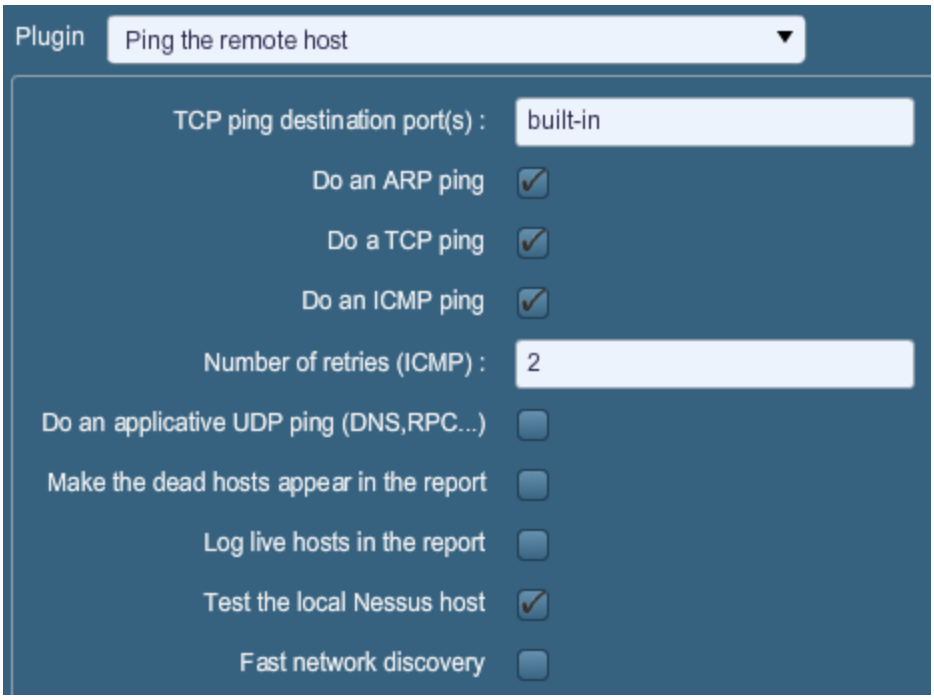
Copyright © 2002-2011 Tenable Network Security, Inc.

Option	Beschreibung
From address (Absenderadresse)	Adresse, die von Nessus für den Versand eines Beitrags an den oder die Newsserver verwendet wird. Der Beitrag selbst wird nach kurzer Zeit automatisch gelöscht.
Test group name regex (Regulärer Ausdruck für Namen der Testgruppen)	Name der Newsgroup(s), die einen Testbeitrag von der angegebenen Adresse erhalten. Der Name kann als regulärer Ausdruck angegeben werden, sodass der Beitrag an mehrere Newsgroups gleichzeitig gesendet werden kann. Beispielsweise wird beim Standardwert „**f[a-z]\.tests?**" ein Beitrag an alle Newsgroups gesendet, deren Name mit einem beliebigen Buchstaben (zwischen „a" und „z") beginnt und auf „.tests" (oder eine dem String entsprechende Abwandlung) endet. Das Fragezeichen dient als optionaler Platzhalter.
Max crosspost (Weiterleitungen maximal)	Maximale Anzahl von Newsservern, die unabhängig von Namensübereinstimmungen den Testbeitrag erhalten. Wenn hier etwa der Wert „**7**" festgelegt wird, wird der Testbeitrag nur an sieben Newsserver gesendet, und zwar auch dann, wenn womöglich 2000 Newsserver dem regulären Ausdruck in diesem Feld entsprechen.
Local distribution (Lokale Übermittlung)	Wenn diese Option ausgewählt ist, sendet Nessus den Testbeitrag nur an lokale Newsserver. Andernfalls wird versucht, den Beitrag auch an vorgeschaltete Systeme weiterzuleiten.
No archive (Keine Archivierung)	Wenn diese Option ausgewählt ist, fordert Nessus an, dass der an die Newsserver gesendete Testbeitrag nicht archiviert wird. Andernfalls wird der Beitrag wie jeder andere auch archiviert.

Unter „**Oracle Settings**" („Oracle-Einstellungen") wird in Nessus die Oracle Database SID konfiguriert. Außerdem wird eine Option zum Testen auf bekannte Standardkonten in der Oracle-Software hinzugefügt.

Bei Auswahl von „**PCI DSS Compliance**" („PCI-DSS-Compliance") kann Nessus die Scanresultate mit den aktuellen Vorgaben für die PCI-DSS-Compliance vergleichen. Diese Funktion steht nur ProfessionalFeed-Kunden zur Verfügung.

Copyright © 2002-2011 Tenable Network Security, Inc.


Plugin
Ping the remote host
TCP ping destination port(s) :
built-in
Do an ARP ping
Do a TCP ping
Do an ICMP ping
Number of retries (ICMP) :
2
Do an applicative UDP ping (DNS,RPC...)
Make the dead hosts appear in the report
Log live hosts in the report
Test the local Nessus host
Fast network discovery

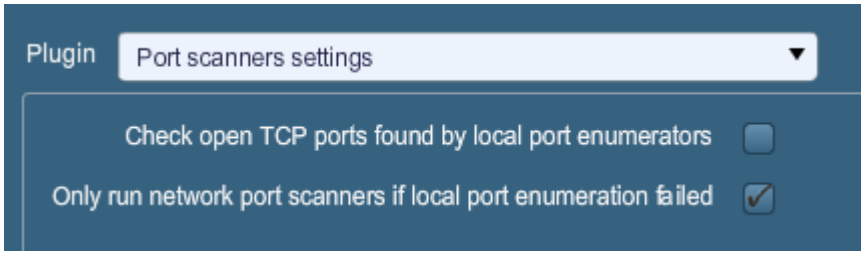
Mit den Optionen unter „**Ping the remote host**" („Pingbefehl an Remotehost senden") lassen sich die Nessus-Funktionen zum Versenden von Pingbefehlen an Hosts während des Erkennungsscans sehr genau konfigurieren. Es können ARP-Pings, TCP-Pings, ICMP-Pings oder geeignete UDP-Pings verwendet werden.

Option	Beschreibung
TCP ping destination port(s) (Zielport(s) für TCP-Pings)	Gibt die Liste der Ports an, die über einen TCP-Ping überprüft werden. Wenn Sie nicht sicher sind, welche Ports Sie angeben sollen, lassen Sie die Voreinstellung „built-in" („Integriert") stehen.
Number of Retries (ICMP) (Anzahl der Wiederholungen (ICMP))	Hiermit können Sie festlegen, wie oft die Übermittlung von Pingbefehlen an den Remotehost probiert wird. Der Standardwert ist „6".
Do an applicative UDP ping (DNS, RPC…) (Geeigneten UDP-Ping ausführen (DNS, RPC …))	Hiermit wird ein UDP-Ping für bestimmte UDP-basierte Anwendungen wie DNS (Port 53), RPC (Port 111), NTP (Port 123) oder RIP (Port 520) ausgeführt.
Make the dead hosts appear in the report (Tote Hosts im Bericht aufführen)	Wenn diese Option aktiviert ist, werden Hosts, die auf die Pinganforderung nicht reagiert haben, als „tote" Hosts im Sicherheitsbericht aufgeführt.
Log live hosts in the report (Hosts, die online sind, im Bericht protokollieren)	Wählen Sie diese Option aus, um im Bericht gezielt aufzuführen, an welche Remotehosts erfolgreich ein Pingbefehl gesendet werden konnte.

Copyright © 2002-2011 Tenable Network Security, Inc.

Test the local Nessus host (Lokalen Nessus-Host testen)	Mithilfe dieser Option können Sie den lokalen Nessus-Host in den Scan einschließen bzw. daraus ausschließen. Die Option wird verwendet, wenn der Nessus-Host in den Bereich des für den Scan konfigurierten Zielnetzwerks fällt.
Fast network discovery (Schnelle Netzwerkerkennung)	Standardmäßig werden, wenn Nessus einen Pingbefehl an eine entfernte IP-Adresse sendet und eine Antwort erhält, zusätzliche Tests durchgeführt, um sicherzustellen, dass es sich nicht um einen transparenten Proxy oder ein Lastausgleichsmodul handelt, von denen statt einer Antwort nur sinnlose Daten zurückgegeben werden (einige Geräte antworten auf jeden Port zwischen 1 und 65.535, auch wenn der betreffende Port von keinem Dienst verwendet wird). Solche Tests können insbesondere dann einige Zeit in Anspruch nehmen, wenn sich der Remotehost hinter einer Firewall befindet. Ist die Option „Fast network discovery" aktiviert, dann werden diese Tests von Nessus nicht ausgeführt.

Zum Scannen von VMware-Gastsystemen muss „ping" deaktiviert sein. Deaktivieren Sie in diesem Fall die Einträge für TCP-, ICMP- und ARP-Pings in der Sicherheitsrichtlinie „Advanced" > „Ping the remote host".


Plugin
Port scanners settings
Check open TCP ports found by local port enumerators
Only run network port scanners if local port enumeration failed

Unter „**Port scanner settings**" („Portscannereinstellungen") sind zwei Optionen für die weitere Steuerung der Portscanneraktivitäten enthalten:

Option	Beschreibung
Check open TCP ports found by local port enumerators (Offene TCP-Ports überprüfen, die von lokalen Port-Enumeratoren gefunden wurden)	Wenn ein lokaler Port-Enumerator (z. B. WMI oder netstat) einen Port erkennt, überprüft Nessus auch, ob dieser Port für Remoteverbindungen geöffnet ist. Auf diese Weise kann festgestellt werden, ob irgendeine Form der Zugriffssteuerung (z. B. TCP-Wrappers, Firewall) verwendet wird.
Only run network port scanners if local port enumeration failed (Netzwerkportscanner nur ausführen, wenn die lokale Port-Enumeration fehlgeschlagen ist)	Andernfalls wird zunächst auf die lokale Port-Enumeration zurückgegriffen.

Copyright © 2002-2011 Tenable Network Security, Inc.

Mit „**SMB Registry: Start the Registry Service during the scan**“ („SMB-Registrierung: Registrierungsdienst während des Scans starten “) kann der Dienst aktiviert werden, um einige Scanvoraussetzungen auf Computern zu erfüllen, auf denen die SMB-Registrierung nicht fortlaufend ausgeführt wird.

Im Menü „**SMB Scope**“ („SMB-Umfang“) werden anstelle lokaler Benutzer Domänenbenutzer abgefragt, sofern die Option „**Request information about the domain**“ („Informationen zur Domäne anfordern“) festgelegt ist.

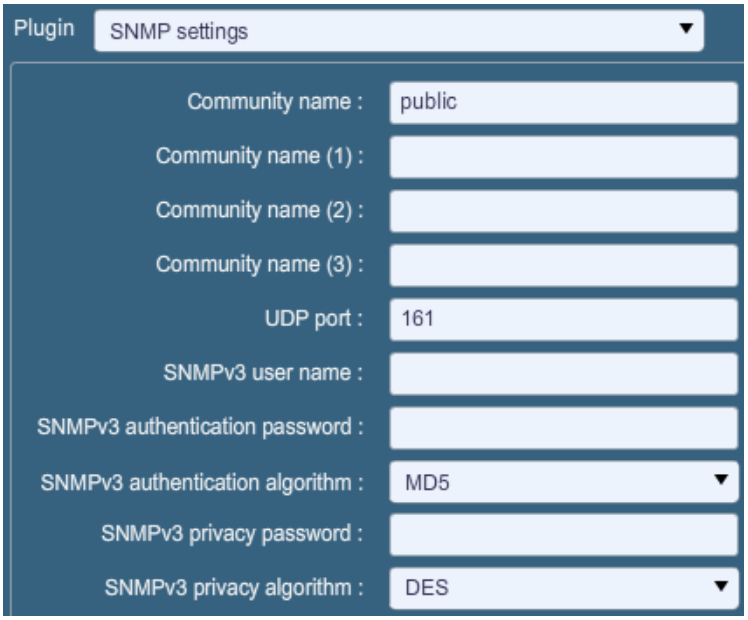
Unter „**SMB Use Domain SID to Enumerate Users**“ („Bei SMB Domänen-SID zur Enumeration von Benutzern verwenden“) wird der SID-Bereich angegeben, für den eine Umkehrsuche (Reverse Lookup) von Benutzernamen in der Domäne ausgeführt wird. Für die meisten Scans wird die Standardeinstellung empfohlen.

Unter „**SMB Use Host SID to Enumerate Users**“ („Bei SMB Host-SID zur Enumeration von Benutzern verwenden“) wird der SID-Bereich angegeben, für den eine Umkehrsuche (Reverse Lookup) lokaler Benutzernamen ausgeführt wird. Die Verwendung der Voreinstellung wird empfohlen.

Unter „**SMTP settings**“ („SMTP-Einstellungen“) werden Optionen für SMTP-Tests (Simple Mail Transport Protocol) angegeben, die auf allen Geräten innerhalb der gescannten Domäne ausgeführt werden, auf denen SMTP-Dienste laufen. Nessus versucht dabei, Meldungen über das Gerät an die unter „**Third party domain**“ angegebene Fremddomäne weiterzuleiten. Wird die an die Fremddomäne gesendete Nachricht von der im Feld „**To address**“ angegebenen Adresse abgewiesen, dann ist der Spamversuch fehlgeschlagen. Wird die Nachricht hingegen akzeptiert, dann wurde der SMTP-Server erfolgreich zur Weiterleitung von Spam verwendet.

Option	Beschreibung
Third party domain (Fremddomäne)	Nessus versucht, Spam über jedes SMTP-Gerät an die in diesem Feld aufgeführte Adresse zu schicken. Die Adresse dieser Fremddomäne muss außerhalb des Bereichs der Site liegen, die gescannt wird bzw. den Scan ausführt. Andernfalls wird der Test durch den SMTP-Server abgebrochen.
From address (Absenderadresse)	Die an den oder die SMTP-Server gesendeten Testnachrichten geben vor, von der in diesem Feld angegebenen Adresse zu stammen.
To address (Empfängeradresse)	Nessus versucht, Nachrichten an die in diesem Feld aufgeführte Empfängeradresse zu schicken. Vorgegeben ist die Adresse **postmaster**, da sie auf den meisten Mailservern gültig ist.

Copyright © 2002-2011 Tenable Network Security, Inc.



Unter „**SNMP settings**" („SNMP-Einstellungen") können Sie Nessus für die Herstellung einer Verbindung mit und die Authentifizierung beim SNMP-Dienst auf dem Zielsystem konfigurieren. Im Verlauf des Scans wird Nessus einige Versuche durchführen, den Community-String zu erraten und für nachfolgende Tests zu verwenden. Je Scanrichtlinie werden bis zu vier separate Community-Strings unterstützt. Kann Nessus den Community-String und/oder das Kennwort nicht erraten, dann kann kein vollständiger Audit des Dienstes ausgeführt werden.

Option	Beschreibung
Community name (0-3) (Community-Name (0-3))	SNMP-Community-Name.
UDP port (UDP-Port)	Weist Nessus an, den Scan über einen anderen Port auszuführen. Vorgesehen für Fälle, in denen SNMP über einen anderen Port als 161 ausgeführt wird.
SNMPv3 user name (SNMPv3-Benutzername)	Benutzername eines SNMPv3-Kontos.
SNMPv3 authentication password (SNMPv3-Authentifizierungskennwort)	Das Kennwort zum angegebenen Benutzernamen.
SNMPv3 authentication algorithm (SNMPv3-Authentifizierungsalgorithmus)	Wählen Sie je nach vom Remotedienst unterstützten Algorithmus MD5 oder SHA1 aus.
SNMPv3 privacy password (SNMPv3-Datenschutzkennwort)	Kennwort, mit dem die verschlüsselte SNMP-Kommunikation geschützt wird.
SNMPv3 privacy algorithm (SNMPv3-Datenschutzalgorithmus)	Der für den SNMP-Datenverkehr verwendete Verschlüsselungsalgorithmus.

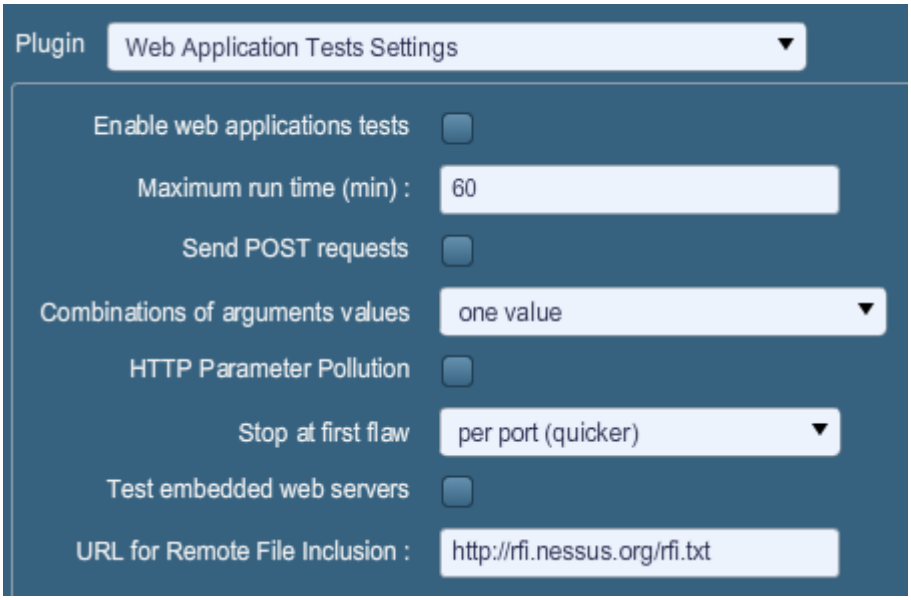
Copyright © 2002-2011 Tenable Network Security, Inc.

Über „**Service Detection**" („Diensterkennung") wird gesteuert, wie Nessus SSL-Dienste testet. Hier können Sie festlegen, ob die Tests für bekannte SSL-Ports (z. B. 443), alle Ports oder gar nicht ausgeführt wird. Das Testen der SSL-Funktionalität auf allen Ports kann auf dem getesteten Host zu einer Betriebsunterbrechung führen.

Über „**Wake-on-LAN**" wird festgelegt, an welche Hosts vor der Ausführung eines Scans WOL-Pakete übermittelt werden sollen und wie lange auf den Start dieser Systeme gewartet werden soll. Die Liste der MAC-Adressen für die WOL-Funktion wird durch den Upload einer Textdatei festgelegt, in der jeweils eine MAC-Adresse pro Zeile aufgeführt ist. Beispiel:

```
00:11:22:33:44:55
aa:bb:cc:dd:ee:ff
[…]
```

Mit der Option „**Unix Compliance Checks**" („UNIX-Compliancetests") können ProfessionalFeed-Kunden UNIX-Auditdateien hochladen, anhand derer ermittelt wird, ob ein getestetes System die angeforderten Compliancestandards erfüllt. Bis zu fünf Richtlinien können gleichzeitig ausgewählt werden.



Über „**Web Application Tests Settings**" („Einstellungen für Webanwendungstests") werden die Argumente der Remote-CGIs (Common Gateway Interface) getestet, die beim Webspiegelungsprozess erkannt wurden. Hierzu wird versucht, verbreitete CGI-Programmierfehler wie Cross-Site Scripting, Remote File Inclusion, Befehlsausführung, Traversal-Angriffe oder SQL Injection zu übergeben. Sie aktivieren diese Option durch Aktivierung des Kontrollkästchens „Enable web applications tests" („Webanwendungstests aktivieren"). Diese Tests erfordern die folgenden NASL-Plugins:

- 11139, 42424, 42479, 42426, 42427, 43160 – SQL Injection (CGI-Missbrauch)
- 39465, 44967 – Befehlsausführung (CGI-Missbrauch)
- 39466, 47831, 42425, 46193, 49067 – Cross-Site Scripting (CGI-Missbrauch: XSS)
- 39467, 46195, 46194 – Directory Traversal (CGI-Missbrauch)
- 39468 – HTTP Header Injection (CGI-Missbrauch: XSS)

Copyright © 2002-2011 Tenable Network Security, Inc.

- 39469, 42056, 42872 –File Inclusion (CGI-Missbrauch)
- 42055 - Formatstring (CGI-Missbrauch)
- 42423, 42054 - Server Side Includes (CGI-Missbrauch)
- 44136 - Cookiemanipulation (CGI-Missbrauch)
- 46196 - XML Injection (CGI-Missbrauch)
- 40406, 48926, 48927 - Fehlermeldungen
- 47830, 47832, 47834, 44134 - Weitere Angriffe (CGI-Missbrauch)

Hinweis: Diese Liste webanwendungsspezifischer Plugins wird regelmäßig aktualisiert. Weitere Plugins können von den hier betroffenen Einstellungen abhängen.

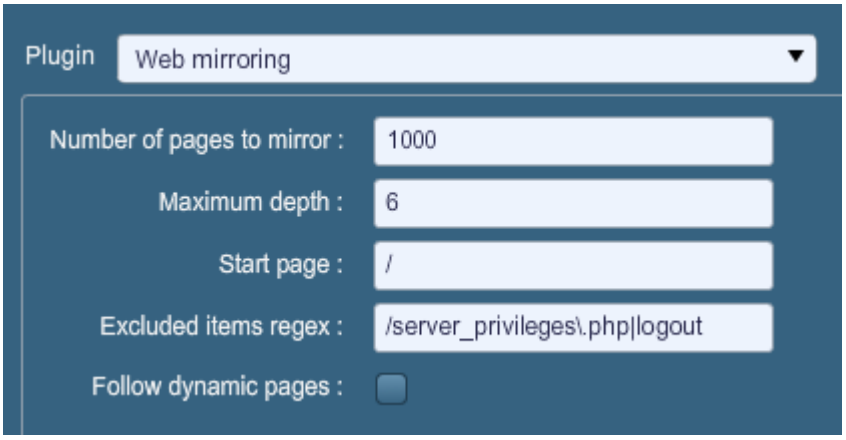
Option	Beschreibung
Maximum run time (min) (Maximale Ausführungszeit (Min.)	Mithilfe dieser Option wird festgelegt, wie viel Zeit für die Durchführung von Webanwendungstests aufgewendet werden darf. Die Vorgabe beträgt 60 Minuten und gilt für alle Ports und CGIs einer Website. Das Scannen des lokalen Netzwerks auf Websites mit kleineren Anwendungen wird in der Regel innerhalb einer Stunde abgeschlossen, doch kann für Websites mit umfangreichen Anwendungen ein höherer Wert erforderlich sein.
Send POST requests (POST-Anforderungen senden)	POST-Anforderungstests werden für erweiterte Tests von Webformularen verwendet. Standardmäßig werden bei Webanwendungstests nur GET-Anforderungen verwendet, sofern diese Option nicht aktiviert ist. Im Allgemeinen verwenden komplexere Anwendungen die POST-Methode, wenn ein Benutzer Daten an die Anwendung übermittelt. Diese Einstellung ermöglicht umfassendere Tests, kann die erforderliche Zeit jedoch erheblich verlängern. Wird sie ausgewählt, dann testet Nessus jedes Skript und jede Variable sowohl mit GET- als auch mit POST-Anforderungen.
Combinations of arguments values (Kombinationen aus Argumentwerten)	Diese Option verwaltet die Kombination von Argumentwerten, die in HTTP-Anforderungen verwendet werden. Das Dropdownmenü enthält drei Optionen: „**One value**" („Bestimmter Wert"): Hiermit wird immer nur ein Parameter gleichzeitig mit einem Angriffsstring getestet. „Angriffslose" Varianten für weitere Parameter werden nicht ausprobiert. Beispielsweise würde Nessus „`/test.php?arg1=XSS&b=1&c=1`" ausprobieren, wobei „b" und „c" andere Werte gestatten würden, ohne dass jede einzelne Kombination überprüft würde. Dies ist die schnellste Testmöglichkeit, bei der zudem die kleinste Ergebnismenge erzeugt wird. „**All pairs (slower but efficient)**" („Alle Paare (langsamer, aber wirkungsvoller)"): Dieser Testansatz ist etwas langsamer, aber wirkungsvoller als der „One value"-Test.

Copyright © 2002-2011 Tenable Network Security, Inc.

	Beim Testen mehrerer Parameter werden ein Angriffsstring und Varianten für eine einzelne Variable getestet, und der erste Wert wird dann für alle anderen Variablen verwendet. Beispielsweise würde Nessus „`/test.php?a=XSS&b=1&c=1&d=1`" ausprobieren und die Variablen dann nacheinander so durchgehen, dass einer Variable der Angriffsstring übergeben wird, einer weiteren zyklisch alle möglichen Werte übergeben werden (wie sie beim Spiegelungsprozess ermittelt wurden) und alle anderen Variablen den ersten Wert erhalten. In diesem Fall würde Nessus etwa niemals auf „`/test.php?a=XSS&b=3&c=3&d=3`" prüfen, wenn der erste Wert jeder Variable „1" wäre. „**All combinations (extremely slow)**" („Alle Kombinationen (extrem langsam)"): Bei dieser Testmethode wird ein umfassender Test aller möglichen Kombinationen von Angriffsstrings mit gültigen Eingabewerten für die Variablen ausgeführt. Hierbei wird bei „All-pairs" („Alle Paare") zur Geschwindigkeitssteigerung versucht, eine kleinere Datenmenge zu erstellen, während bei „All combinations" („Alle Kombinationen") kein Kompromiss eingegangen wird – hier wird die gesamte Datenmenge für Tests verwendet. Beachten Sie, dass der Abschluss des Vorgangs bei dieser Testmethode **sehr lange** dauern kann.
HTTP Parameter Pollution	Beschreibt bei der Durchführung von Webanwendungstests den Versuch, vorhandene Filtermechanismen zu umgehen. Hierzu werden Inhalte in eine Variable injiziert, während gleichzeitig dieselbe Variable mit gültigem Inhalt übergeben wird. Ein normaler SQL-Injektionstest könnte etwa so aussehen: „`/target.cgi?a='&b=2`". Mit aktivierter HTTP Parameter Pollution (HPP) sähe die Anforderung dann eher so aus: „`/target.cgi?a='&a=1&b=2`".
Stop at first flaw (Bei erstem Schwachpunkt anhalten)	Mit dieser Option wird bestimmt, wann ein neuer Schwachpunkt als Ziel verwendet wird. Dies betrifft die Skriptebene: Die Erkennung eines XSS-Schwachpunkts führt nicht zu einer Deaktivierung der Suche nach SQL-Injection- oder Header-Injection-Schwachpunkten; allerdings erhalten Sie maximal einen Bericht zu jedem Typ auf dem jeweiligen Port, sofern „Thorough tests" („Umfassende Tests") nicht festgelegt ist. Beachten Sie, dass mehrere Schwachpunkte desselben Typs z. B. XSS, SQL usw.) gemeldet werden können, sofern sie beim selben Angriff erfasst wurden. Das Dropdownmenü enthält vier Optionen: „**Per CGI** –" („Je CGI"): Sobald ein Schwachpunkt von einem Skript in einem CGI gefunden wurde, wechselt Nessus zum nächsten bekannten CGI auf demselben Server bzw. – wenn kein CGI mehr übrig ist – zum nächsten Port oder Server. Dies ist die Grundeinstellung.

Copyright © 2002-2011 Tenable Network Security, Inc.

	„**Per port (quicker)** –" („Je Port (schneller)"): Sobald ein Schwachpunkt von einem Skript auf einem Webserver gefunden wurde, stoppt Nessus und wechselt zu einem anderen Webserver auf einem anderen Port. „**Per parameter (slow)** –" („Je Parameter (langsam)"): Sobald ein Schwachpunkttyp in einem CGI (z. B. XSS) gefunden wurde, wechselt Nessus zum nächsten Parameter desselben CGI, zum nächsten CGI oder zum nächsten Port oder Server. „**Look for all flaws (slower)** –" („Nach allen Schwachpunkten suchen (langsamer)"): Führt umfassende Tests unabhängig von den gefundenen Schwachpunkten durch. Diese Option kann einen sehr ausführlichen Bericht generieren. In den meisten Fällen ist von ihrer Verwendung abzuraten.
Test Embedded web servers (Eingebettete Webserver testen)	Eingebettete Webserver sind häufig statisch und enthalten keine anpassbaren CGI-Skripts. Zudem sind eingebettete Webserver möglicherweise absturzanfällig oder reagieren beim Scannen nicht mehr. Tenable empfiehlt das Scannen eingebetteter Webserver separat von anderen Webservern mithilfe dieser Option.
URL for Remote File Inclusion (URL für Remote File Inclusion)	Beim RFI-Test (Remote File Inclusion) gibt diese Option eine Datei auf einem Remotehost an, die für die Tests verwendet wird. Standardmäßig benutzt Nessus eine sichere Datei, die auf dem Webserver von Tenable gehostet und speziell für RFI-Tests vorgesehen ist. Kann der Scanner nicht auf das Internet zugreifen, dann wird die Verwendung einer intern gehosteten Datei für genauere RFI-Tests empfohlen.



Mit „**Web Mirroring**" („Webspiegelung") werden Konfigurationsparameter für das native Nessus-Utility zur Spiegelung von Webserverinhalten festgelegt. Nessus spiegelt Webinhalte, um sie besser auf Sicherheitslücken prüfen zu können und die Auswirkungen auf den Server zu minimieren.

Copyright © 2002-2011 Tenable Network Security, Inc.

Wenn die Webspiegelungsparameter so festgelegt sind, dass eine gesamte Website gespiegelt wird, kann dies zu erheblichem Datenaufkommen während des Scans führen. Ist beispielsweise 1 GB Daten auf einem Webserver vorhanden und wurde Nessus so konfiguriert, dass alles gespiegelt wird, so wird beim Scan auch mindestens 1 GB Datenverkehr vom Server zum Nessus-Scanner generiert.

Option	Beschreibung
Number of pages to mirror (Anzahl zu spiegelnder Seiten)	Maximale Anzahl zu spiegelnder Seiten.
Maximum depth (Maximale Spiegelungstiefe)	Hiermit wird angegeben, wie vielen Links Nessus je Startseite folgt.
Start page (Startseite)	URL der ersten zu testenden Seite. Sind mehrere Seiten erforderlich, dann können diese durch einen Doppelpunkt getrennt angegeben werden (z. B. „/:/php4:/base“).
Excluded items regex (Regulärer Ausdruck für ausgeschlossene Elemente)	Hiermit wird der Ausschluss von Teilen der erfassten Website aktiviert. Um beispielsweise das Verzeichnis „/manual“ und alle Perl-CGIs auszuschließen, geben Sie folgenden Wert für dieses Feld an: **(^/ manual) | (\ . pl (\ ?. *) ?$) .**
Follow dynamic pages (Dynamischen Seiten folgen)	Wenn diese Option aktiviert ist, folgt Nessus dynamischen Links, wodurch die oben festgelegten Grenzwerte überschritten werden können.

Mit der Option „**Windows Compliance Checks**“ („Windows-Compliancetests“) können ProfessionalFeed-Kunden Windows-Konfigurationsauditdateien hochladen, anhand derer ermittelt wird, ob ein getestetes System die angeforderten Compliancestandards erfüllt. Bis zu fünf Richtlinien können gleichzeitig ausgewählt werden.

Mit der Option „**Windows File Contents Compliance Checks**“ können ProfessionalFeed-Kunden Windows-basierte Auditdateien hochladen, die nach bestimmten Inhaltstypen suchen (z. B. Kreditkarten, Social Security-Nummern usw.), und so die Compliance in Bezug auf Unternehmensrichtlinien oder Drittvorgaben bestimmen.

Wenn alle Optionen wie gewünscht konfiguriert wurden, klicken Sie auf „**Submit**“ („Absenden“), um die Richtlinie zu speichern und zur Registerkarte „Policies“ zurückzukehren. Sie können jederzeit auf „**Edit**“ („Bearbeiten“) klicken, um Änderungen an einer Richtlinie vorzunehmen, die Sie bereits erstellt haben. Durch Anklicken von „**Delete**“ löschen Sie eine Richtlinie vollständig.

Richtlinien importieren, exportieren und kopieren

Über die Schaltfläche „**Import**“ oben rechts in der Menüleiste können Sie zuvor erstellte Richtlinien in den Scanner hochladen. Wählen Sie über das Dialogfeld „**Browse...**“ („Durchsuchen“) die Richtlinie auf Ihrem lokalen System aus und klicken Sie auf „**Submit**“ („Absenden“).

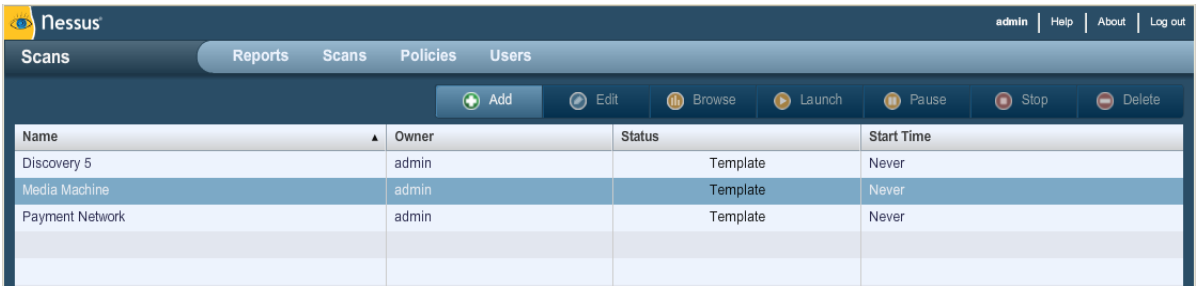
Copyright © 2002-2011 Tenable Network Security, Inc.

Über die Schaltfläche „**Export**“ oben rechts in der Menüleiste können Sie eine bestehende Richtlinie aus dem Scanner in das lokale Dateisystem herunterladen. Im Downloaddialogfeld des Browsers können Sie angeben, dass die Richtlinie in einem externen Programm (z. B. dem Texteditor) geöffnet oder in einem frei wählbaren Verzeichnis gespeichert wird.

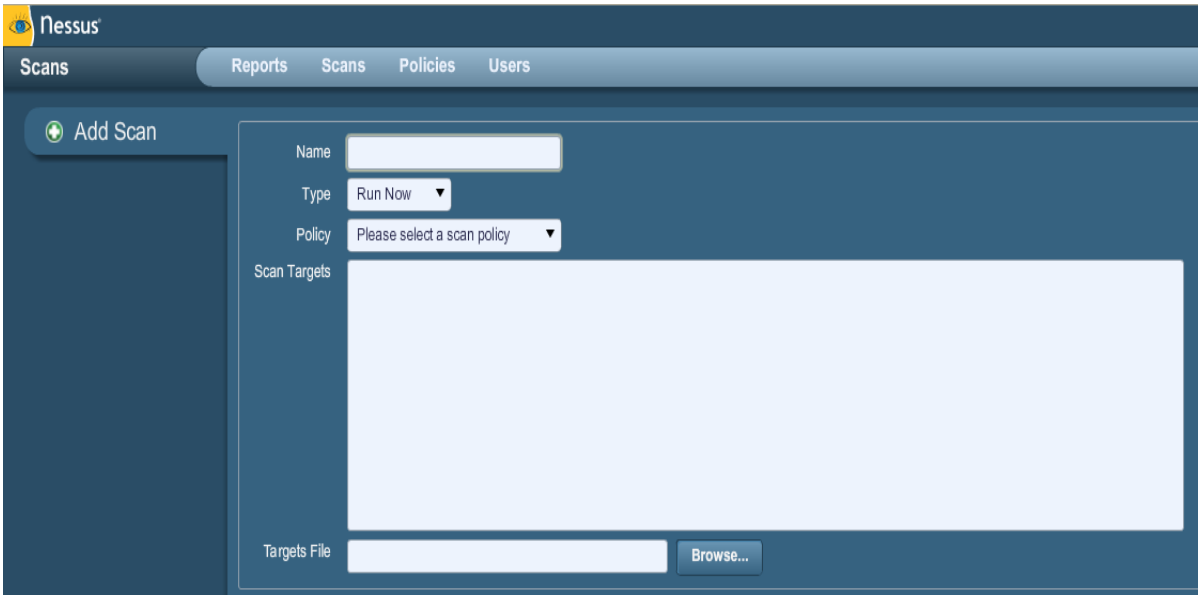
Kennwörter und `.audit`-Dateien, die in einer Richtlinie enthalten sind, werden **nicht** exportiert.

Wenn Sie eine Richtlinie erstellen möchten, die im Vergleich zu einer vorhandenen Richtlinie nur kleinere Änderungen aufweist, können Sie die Ausgangsrichtlinie in der Liste auswählen und dann oben rechts in der Menüleiste auf „**Copy**“ („Kopieren“) klicken. Hierdurch wird eine Kopie der Ausgangsrichtlinie erstellt, die bearbeitet werden kann, um die erforderlichen Änderungen vorzunehmen. Dies ist sinnvoll zur Erstellung von Standardrichtlinien mit geringfügigen Änderungen, wie sie in der jeweiligen Umgebung erforderlich sind.

SCANS ERSTELLEN, STARTEN UND PLANEN


Nessus
admin | Help | About | Log out
Scans
Reports Scans Policies Users
Add Edit Browse Launch Pause Stop Delete
Name Owner Status Start Time
Discovery 5 admin Template Never
Media Machine admin Template Never
Payment Network admin Template Never

Wenn Sie eine Richtlinie erstellt haben, können Sie einen neuen Scan anlegen. Klicken Sie hierzu auf die Option „**Scans**“ oben in der Menüleiste und dann rechts auf die Schaltfläche „**+ Add**“ („Hinzufügen“). Das Fenster „**Add Scan**“ („Scan hinzufügen“) erscheint:



Copyright © 2002-2011 Tenable Network Security, Inc.

Hier sind fünf Felder zur Eingabe des Scanziels vorhanden:

- **Name**: Hier wird der Name festgelegt, der zur Bezeichnung des Scans auf der Nessus-Benutzeroberfläche verwendet wird.
- **Type** (Typ): Wählen Sie „Run Now" („Jetzt ausführen"; führt den Scan unmittelbar nach der Eingabe aus), „Scheduled" („Geplant"; erlaubt die Festlegung des Zeitpunkts, zu dem der Scan gestartet werden soll) oder „Template" („Vorlage"; speichert die Eingaben als Vorlage für wiederholbare Scans).
- **Policy** (Richtlinie): Wählen Sie eine zuvor erstellte Richtlinie aus, anhand derer die Parametereinstellungen für den Scan vorgenommen werden. Mit diesen wird das Verhalten des Nessus-Serverscanners kontrolliert.
- **Scan Targets** („Scanziele"): Ziele können als einzelne IP-Adresse (z. B. „192.168.0.1"), als IP-Bereich (z. B. „192.168.0.1-192.168.0.255"), als Subnetz in CIDR-Notation (z. B. „192.168.0.0/24") oder als auflösbarer Host (z. B. „www.nessus.org") angegeben werden.
- **Targets File** (Zieldatei): Eine Textdatei, die eine Liste mit Hosts enthält, kann durch Anklicken von „**Browse...**" und nachfolgende Auswahl der Datei auf dem lokalen Computer festgelegt werden.

Die Hostdatei muss als ASCII-Text formatiert sein. Pro Zeile muss ein Host angegeben sein, und es dürfen weder Leerzeichen noch Leerzeilen vorhanden sein. Die Unicode-/UTF-8-Kodierung wird nicht unterstützt.

Beispiel für Hostdateiformate:

Einzelne Hosts:

```
192.168.0.100
192.168.0.101
192.168.0.102
```

Hostbereich:

```
192.168.0.100-192.168.0.102
```

Hostblock in CIDR-Notation:

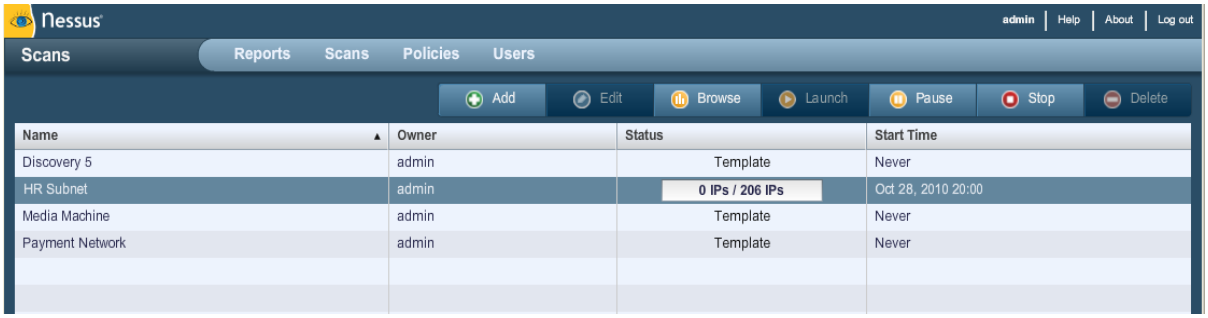
```
192.168.0.1/24
```

Virtuelle Server:

```
www.tenable.com[192.168.1.1]
www.nessus.org[192.168.1.1]
www.tenablesecurity.com[192.168.1.1]
```

Nachdem Sie die Scaninformationen angegeben haben, klicken Sie auf „**Submit**". Nach der Übertragung beginnt der Scan sofort, sofern Sie zuvor „Run Now" ausgewählt haben. Erst nach Abschluss des Scans wird wieder die allgemeine Seite „**Scans**" angezeigt.

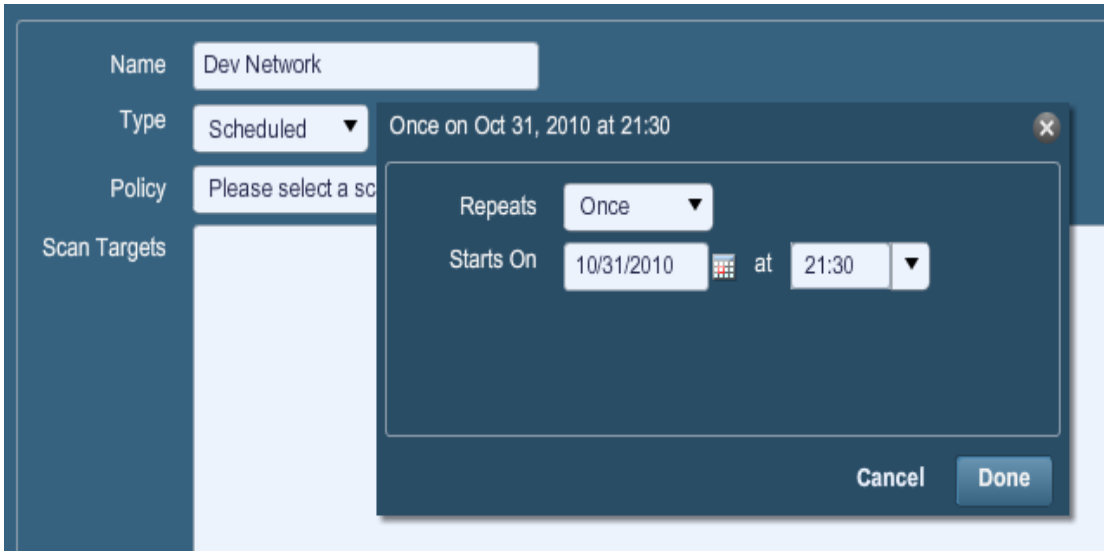
Copyright © 2002-2011 Tenable Network Security, Inc.



Nach dem Starten des Scans zeigt die Liste „Scans" alle gegenwärtig ausgeführten, unterbrochenen oder als Vorlage ausgewählten Scans sowie zugehörige Basisinformationen an. Nach Auswahl eines bestimmten Scans aus der Liste können Sie über die Schaltflächen oben rechts die laufenden Scanergebnisse durchsuchen („**Browse**"), den Scan unterbrechen („**Pause**") und fortsetzen („**Resume**"), ihn beenden („**Stop**") und bei Bedarf vollständig löschen („**Delete**"). Außerdem können Benutzer Scanvorlagen nach Anklicken der Schaltfläche „**Edit**" bearbeiten.

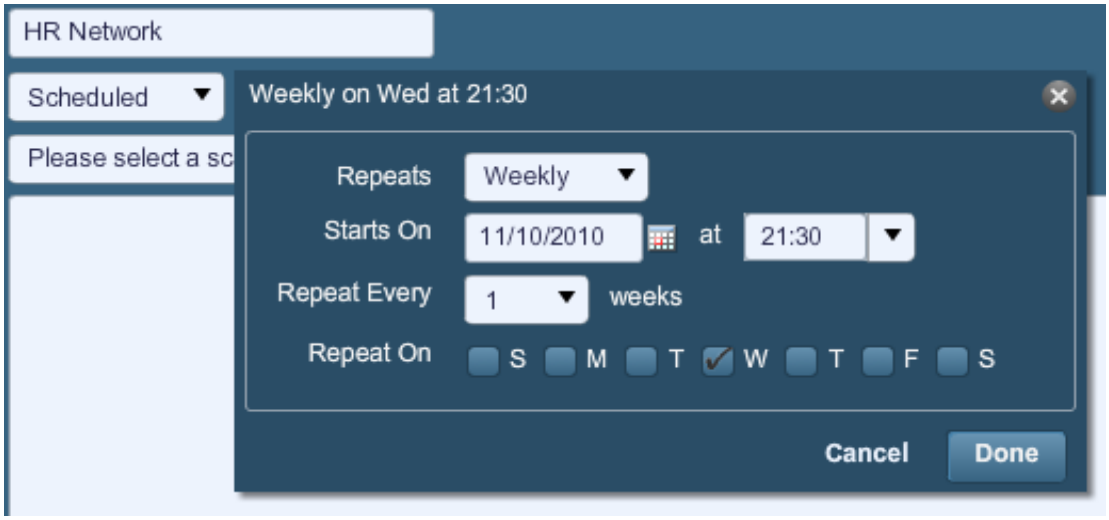
Wenn ein Scan (auf welche Weise auch immer) beendet wurde, wird er aus der Liste „**Scans**" entfernt. Gleichzeitig erscheint er zur Kontrolle auf der Registerkarte „**Reports**".

Wurde ein Scan geplant („Scheduled"), dann werden Optionen zur Eingabe der gewünschten Startzeit und der Häufigkeit angezeigt:



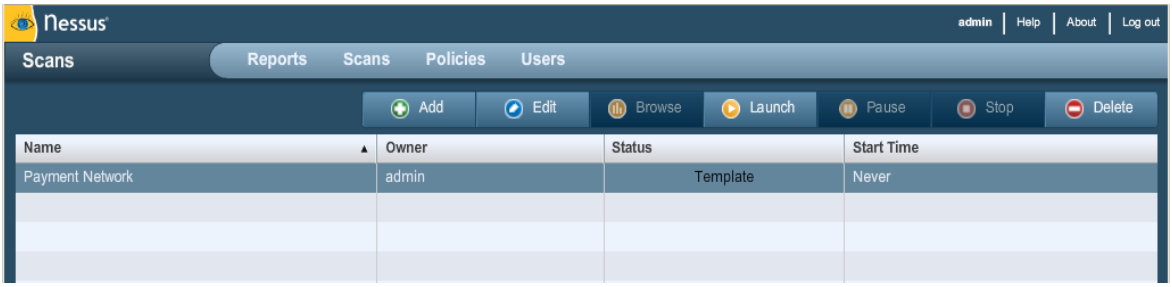
Über das Dropdownmenü „Repeats" („Wiederholungen") können Sie festlegen, ob ein Scan einmalig, täglich, wöchentlich, monatlich oder jährlich ausgeführt wird. Für die hier getroffene Auswahl kann zudem ein Startzeitpunkt (Datum und Uhrzeit) festgelegt werden. Ist der Scan gespeichert, dann wird er von Nessus zum gewünschten Zeitpunkt gestartet.

Copyright © 2002-2011 Tenable Network Security, Inc.



Maßgeblich für die Scanstartzeit ist die Zeiteinstellung auf dem Nessus-Scannerserver.

Wurde ein Scan als Vorlage gespeichert, dann wird er in der Scanliste auch als solche angezeigt und kann gestartet werden.



Die Möglichkeit der Zeitplanung von Scans steht nur ProfessionalFeed-Kunden zur Verfügung.

Berichte

Seit Nessus 4.2 sind Berichts-Stylesheets besser in das Berichterstellungssystem integriert. Mithilfe von Berichtsfiltern und Exportfunktionen kann der Benutzer dynamische Berichte nach eigenen Prioritäten erstellen, statt lediglich aus einer Liste vorgefertigter Berichte wählen zu können. Außerdem wurde die Unterstützung von Stylesheets erweitert, sodass Updates ebenso wie Ergänzungen bei den Stylesheets über den Plugin-Feed erfolgen können. Dies ermöglicht Tenable die Veröffentlichung weiterer Stylesheets auch ohne erforderliches Upgrade oder Einführung einer neuen Hauptversion.

Wenn Sie oben auf der Benutzeroberfläche auf die Registerkarte „**Reports**“ („Berichte“) klicken, wird eine Liste mit laufenden und abgeschlossenen Scans angezeigt:

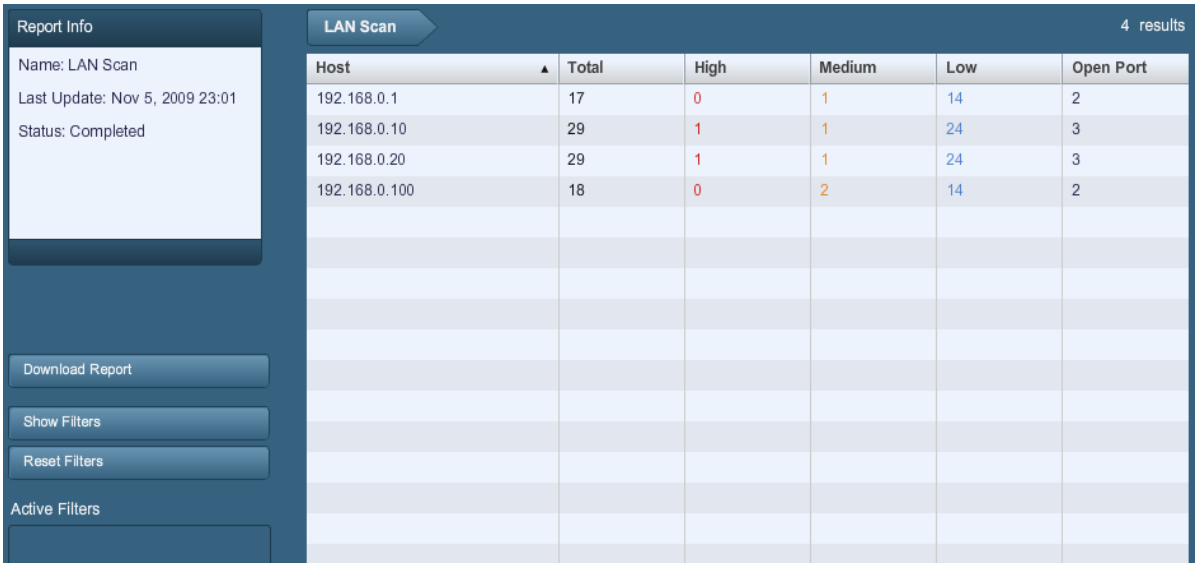
Copyright © 2002-2011 Tenable Network Security, Inc.

Nessus
admin | Help | About | Log out
Reports
Reports Scans Policies Users
Browse Compare Upload Download Delete
Name Status Last Updated
Dev Subnet Completed Nov 3, 2009 24:35
HR Subnet Running Nov 3, 2009 24:38
Local Desktop Completed Nov 3, 2009 24:40

Der Bildschirm „Reports" („Berichte") ist die zentrale Anlaufstelle zum Anzeigen, Vergleichen, Hochladen und Herunterladen von Scanergebnissen. Mithilfe der Umschalt- oder der STRG-Taste können Sie mehrere Berichte gleichzeitig auswählen.

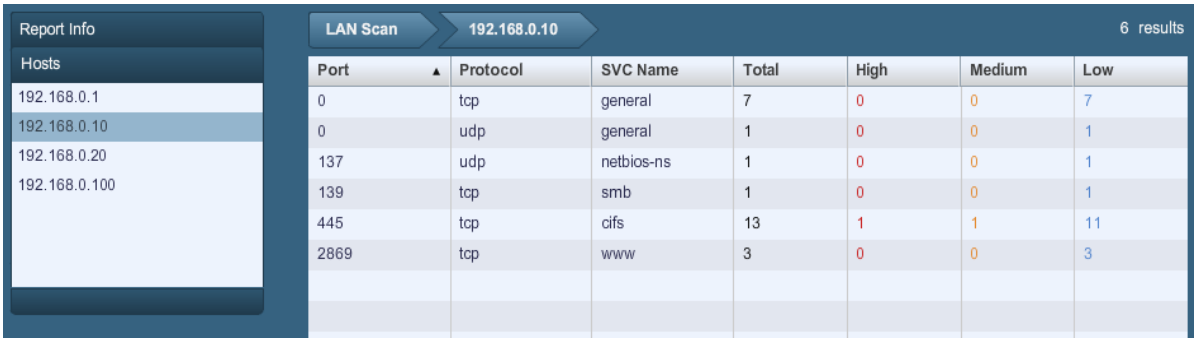
Browse (Durchsuchen)

Wählen Sie zum Durchsuchen der Ergebnisse eines Scans einen Namen aus der Liste „Reports" aus und klicken auf „**Browse**". Nun können Sie die unterschiedlichen Resultate anzeigen, indem Sie zu Hosts, Ports und dann bestimmten Sicherheitslücken navigieren. Der erste Zusammenfassungsbildschirm zeigt alle gescannten Hosts sowie in einer Übersicht die gefundenen Sicherheitslücken und offenen Ports an:



Wählen Sie einen Host aus, so wird der Bericht nach Portnummern unterteilt und zeigt zugehörige Informationen wie beispielsweise das Protokoll und den Dienstnamen sowie eine nach Risiko gegliederte Zusammenfassung der Sicherheitslücken. Während Sie die Scanresultate durchsehen, bleibt die Liste der Hosts weiterhin auf der Benutzeroberfläche angezeigt. Ferner ist eine Anzahl anklickbarer Pfeile vorhanden, die eine schnelle Navigation zu einer bestimmten Komponente des Berichts ermöglichen:

Copyright © 2002-2011 Tenable Network Security, Inc.



Bei Auswahl eines Ports werden alle dem Port und dem zugehörigen Dienst zugeordneten gefundenen Sicherheitslücken aufgelistet:

LAN Scan
192.168.0.10
445 / tcp
List
Detail
13 results
Plugin ID
Name
Port
Severity
11011 SMB Detection cifs (445/tcp) Low
10785 SMB NativeLanMan cifs (445/tcp) Low
10394 SMB log in cifs (445/tcp) Low
10859 SMB get host SID cifs (445/tcp) Low
10860 SMB use host SID to enumerate local users cifs (445/tcp) Low
10395 SMB shares enumeration cifs (445/tcp) Low
26919 SMB guest account for all users cifs (445/tcp) Medium
10397 SMB LanMan Pipe Server browse listing cifs (445/tcp) Low
10396 Microsoft Windows SMB Shares Access cifs (445/tcp) High
23974 SMB Share Hosting Office Files cifs (445/tcp) Low
10400 SMB accessible registry cifs (445/tcp) Low
10428 SMB fully accessible registry cifs (445/tcp) Low
26920 SMB NULL session cifs (445/tcp) Low

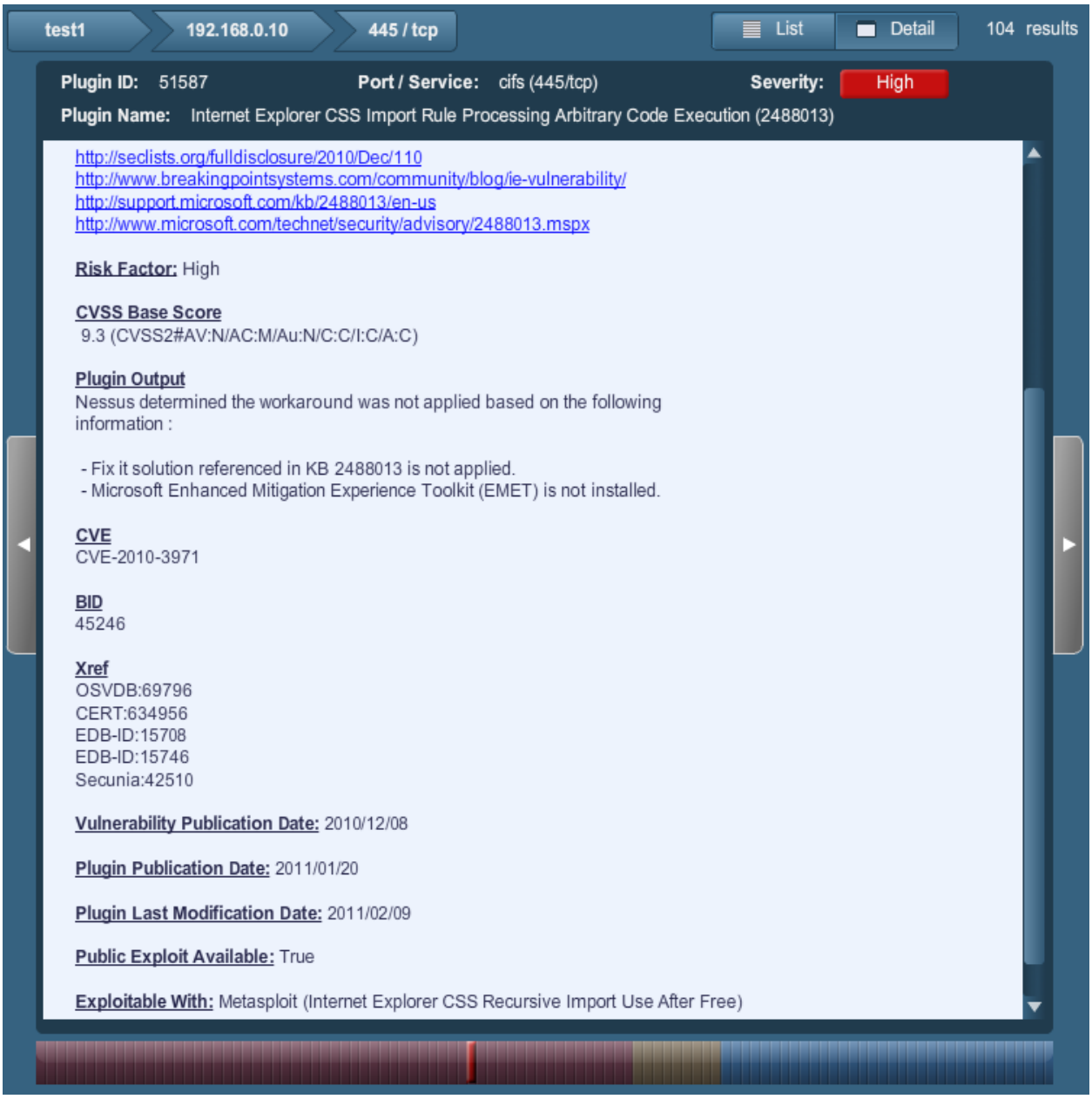
Im obigen Beispiel sehen wir, dass der Host 192.168.0.10 insgesamt 13 Sicherheitslücken über den TCP-Port 445 (CIFS, Common Internet File System) aufweist. In der Ergebniszusammenfassung sind die ID des Nessus-Plugins, der Name der Sicherheitslücke, der Port, das Protokoll und der Schweregrad aufgeführt. Durch Anklicken der Spaltenüberschriften können die Ergebnisse entsprechend dem Inhalt der betreffenden Spalte sortiert werden. Durch erneutes Anklicken wird die Sortierreihenfolge umgekehrt:

Copyright © 2002-2011 Tenable Network Security, Inc.

Plugin ID	Name	Port	Severity
10396	Microsoft Windows SMB Shares Access	cifs (445/tcp)	High
26919	SMB guest account for all users	cifs (445/tcp)	Medium
10397	SMB LanMan Pipe Server browse listing	cifs (445/tcp)	Low
10859	SMB get host SID	cifs (445/tcp)	Low
10860	SMB use host SID to enumerate local users	cifs (445/tcp)	Low
10395	SMB shares enumeration	cifs (445/tcp)	Low
11011	SMB Detection	cifs (445/tcp)	Low
10394	SMB log in	cifs (445/tcp)	Low
10785	SMB NativeLanMan	cifs (445/tcp)	Low
23974	SMB Share Hosting Office Files	cifs (445/tcp)	Low
10400	SMB accessible registry	cifs (445/tcp)	Low
10428	SMB fully accessible registry	cifs (445/tcp)	Low
26920	SMB NULL session	cifs (445/tcp)	Low

Wenn Sie eine Sicherheitslücke aus der Liste auswählen, werden alle zugehörigen Details angezeigt: eine Kurzzusammenfassung, eine technische Beschreibung, die Lösung, der Risikofaktor, die CVSS-Bewertung, die als Nachweis des Resultats verwendete relevante Ausgabe, externe Verweise, Veröffentlichungsdatum der Sicherheitslücke, Veröffentlichungs- oder Änderungsdatum des zugehörigen Plugins und Informationen zur Verfügbarkeit von Exploits:

Copyright © 2002-2011 Tenable Network Security, Inc.



Am Ende werden alle bekannten, öffentlich verfügbaren Exploits für die Sicherheitslücke angezeigt. Dies schließt auch solche mit ein, die in (öffentlich verfügbaren oder kommerziellen) Sicherheitslücken-Frameworks wie CANVAS, CORE oder Metasploit zu finden sind.

Im Detailfenster sind mehrere Möglichkeiten zur Navigation im Bericht vorhanden:

- Die Pfeilschaltflächen ganz oben im Fenster ermöglichen die Rückkehr zu einem Port, einem Host oder zur Scanübersicht.
- Mit den Schaltflächen „**List**" („Liste") und „**Detail**" schalten Sie zwischen der Detailansicht zur Sicherheitslücke und der letzten Listenansicht (im obigen Beispiel etwa die zu Port 445 gehörenden Sicherheitslücken) um.

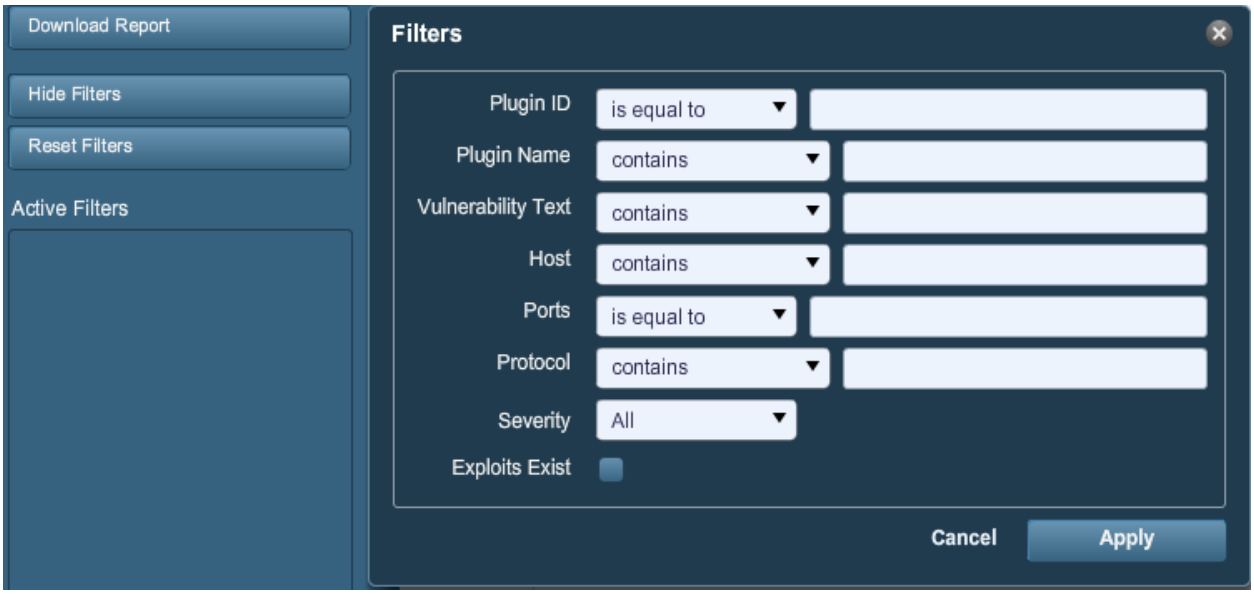
Copyright © 2002-2011 Tenable Network Security, Inc.

- Mit den grauen Links- und Rechtspfeilen rufen Sie die anderen mit dem ausgewählten Port verknüpften Sicherheitslücken nacheinander auf.
- Die Schaltflächenleiste am unteren Fensterrand erlaubt den direkten, nach Schweregrad abgestuften Aufruf einer bestimmten Sicherheitslücke in der Liste. Im obigen Beispiel sind die mit mittelschweren und schweren Risiken behafteten Sicherheitslücken hervorgehoben.

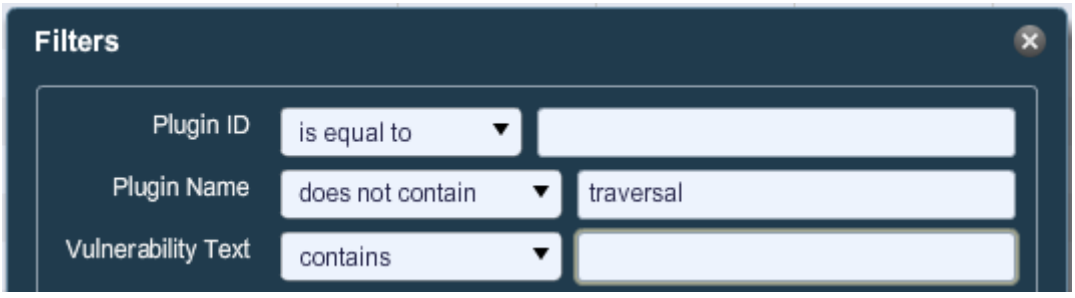
Berichtsfilter

Nessus bietet ein flexibles Filtersystem, mit dem die Anzeige bestimmter Berichtsresultate vereinfacht wird. Mithilfe von Filtern lassen sich Ergebnisse basierend auf jedem beliebigen Aspekt der gefundenen Sicherheitslücken anzeigen. Werden mehrere Filter verwendet, dann lassen sich detaillierte und angepasste Berichtsansichten erstellen.

Klicken Sie zur Erstellung eines Filters zunächst links auf dem Bildschirm auf „**Show Filters**" („Filter anzeigen"). Filter lassen sich aus der Berichtszusammenfassung oder den Übersichtsbildschirmen auf der Host- und der Portebene erstellen.



Ein Filter wird erstellt, indem das Feld, ein Filterargument und ein zu filternder Wert ausgewählt werden:



Copyright © 2002-2011 Tenable Network Security, Inc.

Die Berichtsfilter unterstützen eine Vielzahl von Kriterien:

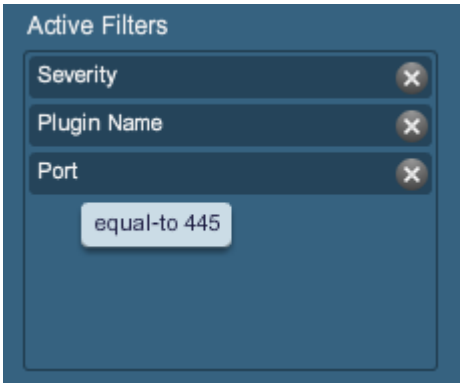
Option	Beschreibung
Plugin ID (Plugin-ID)	Filtert Ergebnisse, wenn die Plugin-ID einer bestimmten Zahl (z. B. 42111) entspricht („*is equal to*“) bzw. nicht entspricht („*is not equal to*“).
Plugin Name (Plugin-Name)	Filtert Ergebnisse, wenn der Plugin-Name einen gegebenen String (z. B. „Microsoft Windows“) enthält („*contains*“), nicht enthält („*does not contain*“), mit diesem beginnt („*starts with*“) oder nicht mit diesem beginnt („*does not start with*“).
Vulnerability Text (Sicherheitslückentext)	Filtert Ergebnisse, wenn die Plugin-Ausgabe einen bestimmten String (z. B. „Denial of Service“) enthält („*contains*“), nicht enthält („*does not contain*“), mit diesem beginnt („*starts with*“) oder nicht mit diesem beginnt („*does not start with*“).
Host	Filtert Ergebnisse, wenn der Host einen bestimmten String (z. B. „192.168“) enthält („*contains*“), nicht enthält („*does not contain*“), mit diesem beginnt („*starts with*“), nicht mit diesem beginnt („*does not start with*“), diesem entspricht („*is equal to*“) oder diesem nicht entspricht („*is not equal to*“).
Ports	Filtert Ergebnisse basierend darauf, ob ein Port einer bestimmten Zahl (z. B. 443) entspricht („*is equal to*“) bzw. nicht entspricht („*is not equal to*“).
Protocol (Protokoll)	Filtert Ergebnisse, wenn ein Protokoll einen bestimmten String (z. B. „http”) enthält („*contains*”), nicht enthält („*does not contain*”), mit diesem beginnt („*starts with*”) oder nicht mit diesem beginnt („*does not start with*”).
Severity (Schweregrad)	Filtert Ergebnisse basierend auf dem Schweregrad des Risikos: niedrig („*Low*“), moderat („*Medium*“), hoch („*High*“) oder kritisch („*Critical*“). Die Schweregradbewertungen sind von der zugehörigen CVSS-Bewertung abgeleitet. Dabei wird eine Punktzahl von unter 5 als „niedrig“, unter 7 als „moderat“, unter 10 als „hoch“ und von 10 oder höher als „kritisch“ gewertet.
Exploits Exist (Exploits vorhanden)	Filtert je nachdem, ob für die betreffende Sicherheitslücke ein Exploit existiert.

Bei der Verwendung eines Filters kann der String bzw. der Zahlenwert auch kommagetrennt sein, um nach mehreren Strings zu filtern. Um beispielsweise nur Ergebnisse anzuzeigen, die sich auf Webserver beziehen, könnten Sie einen Filter „Ports“ erstellen, als Filterbedingung „is equal to“ und als Eingabewert „80,443,8000,8080“ festlegen. Auf diese Weise werden Ihnen nur Ergebnisse zu diesen vier Ports angezeigt.

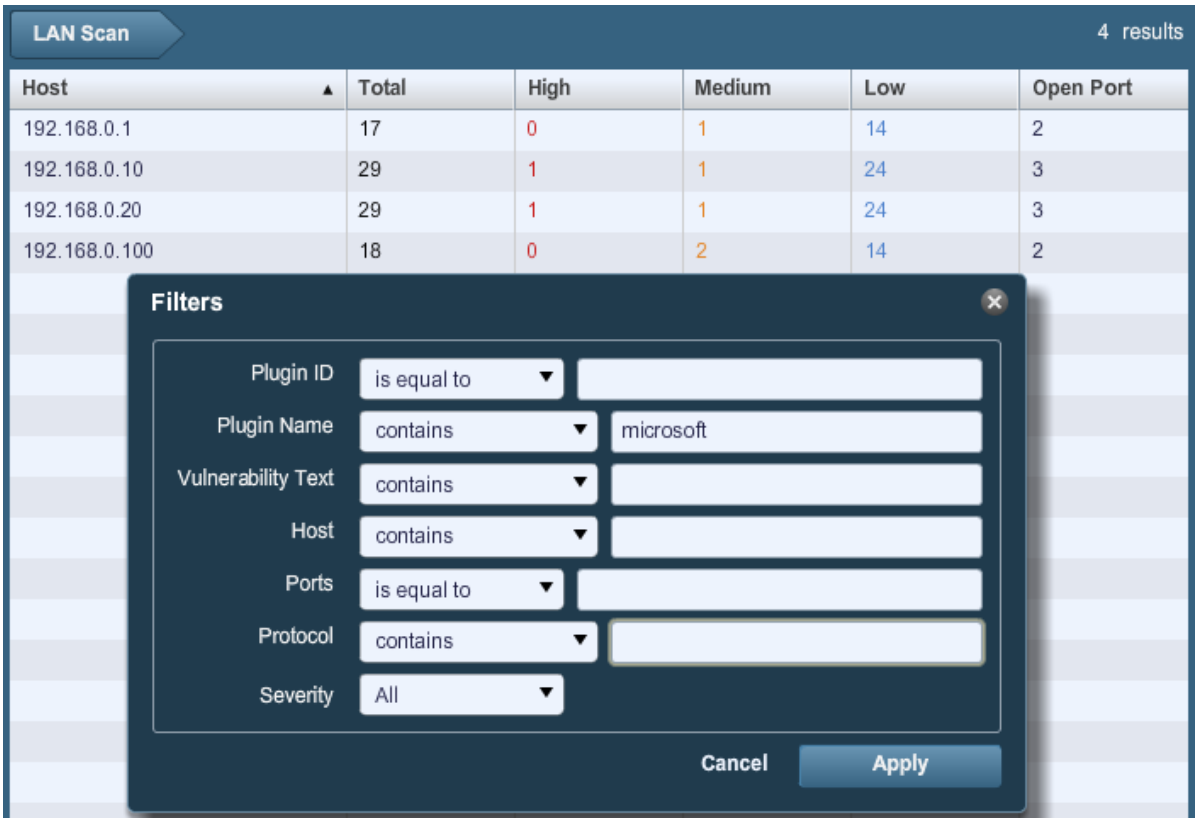
Copyright © 2002-2011 Tenable Network Security, Inc.

Bei Filterkriterien wird die Groß-/Kleinschreibung **nicht** beachtet.

Nach ihrer Erstellung erscheinen Filter in der Liste auf der linken Seite. Um die aktiven Filterdetails anzuzeigen, setzen Sie den Cursor auf den Filternamen:



Sobald ein Filter erstellt ist, werden die Scanergebnisse entsprechend den neuen Filterkriterien aktualisiert. Im nachfolgenden Beispiel werden durch Erstellung eines Filters, der nur Ergebnisse mit dem String „Microsoft" im Plugin-Namen anzeigt, die meisten Ergebnisse entfernt:



Copyright © 2002-2011 Tenable Network Security, Inc.

Nach Anwendung des Filters:

Wenn die Ergebnisse so gefiltert wurden, dass die von Ihnen gewünschten Daten angezeigt werden, können Sie auf „**Download Report**" („Bericht herunterladen") klicken, um nur die gefilterten Ergebnisse zu exportieren.

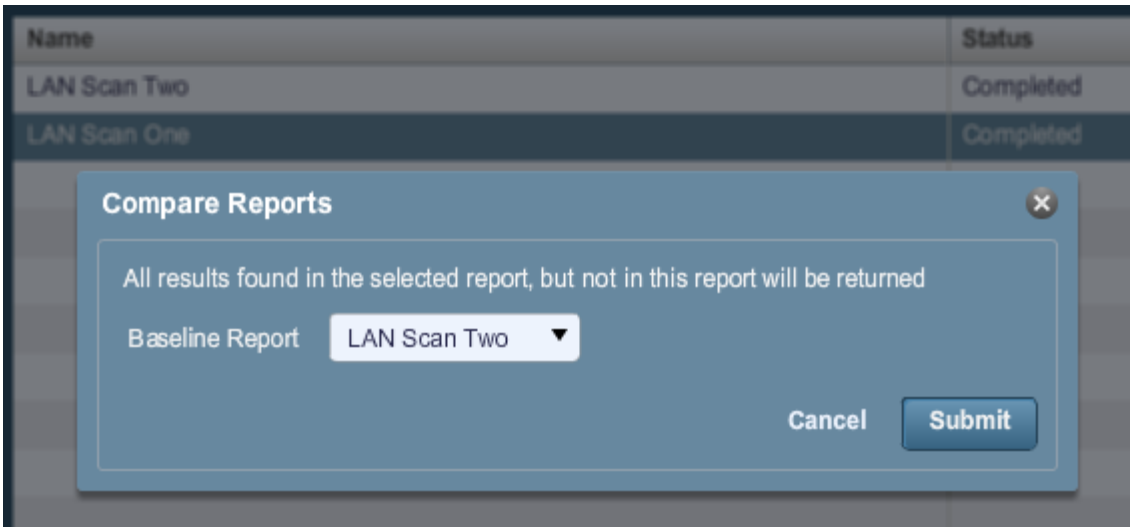
Compare (Vergleichen)

Die Funktion „Compare" steht nur ProfessionalFeed-Benutzern zur Verfügung.

Ab Nessus 4.4 können Sie zwei Scanberichte miteinander vergleichen, um Unterschiede anzuzeigen. Durch die Möglichkeit, Unterschiede zwischen Scans anzuzeigen, lässt sich feststellen, wie sich das jeweilige System oder Netzwerk im Laufe der Zeit verändert hat. Dies erleichtert Compliance-Analysen, denn Sie können so erkennen, welche Sicherheitslücken geschlossen wurden, ob Systeme bei Feststellung neuer Sicherheitslücken entsprechend gepatcht wurden oder dass zwei Scans möglicherweise nicht die gleichen Hosts verarbeiten.

Wählen Sie zum Vergleich von Berichten zunächst einen Scan aus der Liste „**Reports**" aus und klicken dann in der Menüleiste rechts auf „**Compare**". Das resultierende Dialogmenü enthält eine Dropdownliste mit anderen Berichten, die verglichen werden können. Wählen Sie einen Bericht aus und klicken Sie auf „**Submit**":

Copyright © 2002-2011 Tenable Network Security, Inc.



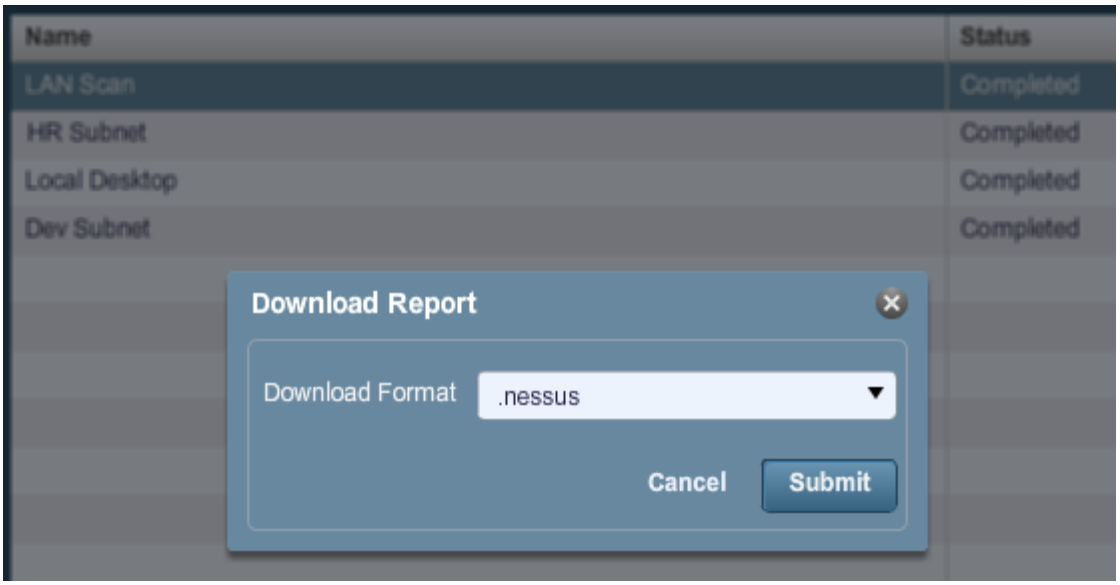
Nessus vergleicht die beiden Berichte und generiert eine Liste mit Ergebnissen, die nicht in beiden Berichten enthalten sind. Diese Ergebnisse sind die Unterschiede zwischen den Scans. An ihnen lässt sich ablesen, welche Sicherheitslücken zwischen den beiden Scans gefunden bzw. behoben wurden. Im obigen Beispiel ist „LAN Scan One" ein Scan des gesamten Subnetzes 192.168.0.0/24 und „LAN Scan Two" ein Scan dreier ausgewählter Hosts im selben Subnetz. Die Funktion „Compare" zeigt die Unterschiede an, indem Hosts, die in „LAN Scan Two" nicht gescannt wurden, hervorgehoben werden:

Upload und Download

Scanergebnisse können aus einem Scanner exportiert und in einen anderen importiert werden. Die Funktionen „**Upload**" und „**Download**" erleichtern Scanmanagement, Berichtsvergleich, Sicherung von Berichten und die Kommunikation zwischen Gruppen und Organisationen innerhalb eines Unternehmens.

Wählen Sie den zu exportierenden Scan aus der Liste „**Reports**" aus und klicken Sie auf „**Download**". Nun wird das Dialogfeld zum Herunterladen von Berichten angezeigt:

Copyright © 2002-2011 Tenable Network Security, Inc.



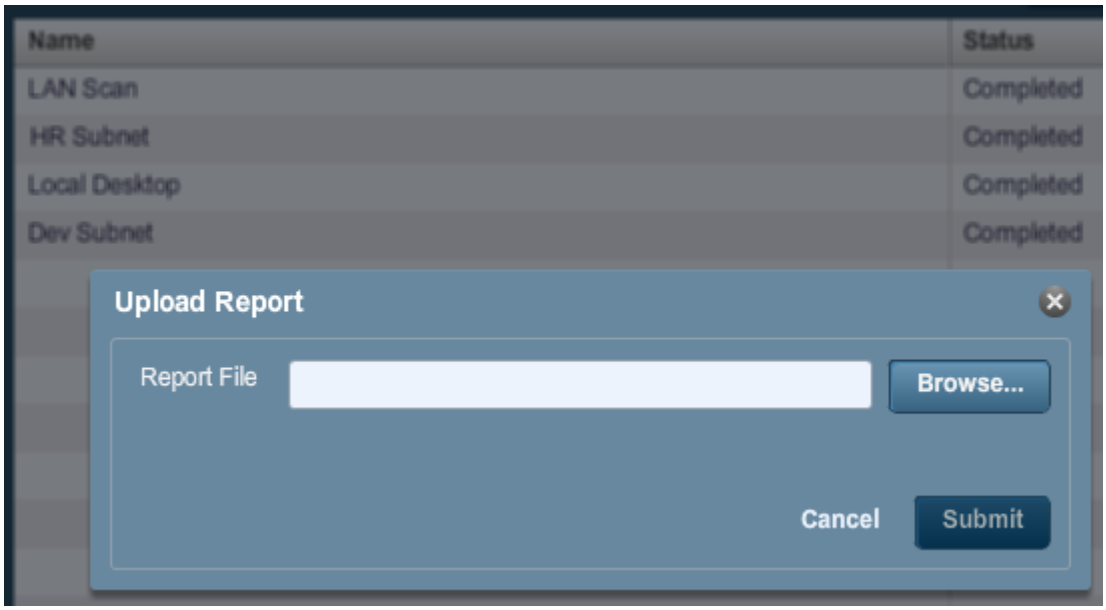
Berichte können in einem von vier Formaten heruntergeladen werden:

Option	Beschreibung
`.nessus`	Dieses XML-basierte Format ist der De-facto-Standard in Nessus 4.2 und höher. Es verwendet einen erweiterten Satz XML-Tags, um das Extrahieren und Analysieren von Informationen granularer zu gestalten.
`.nessus` **(v1)**	Ein XML-basiertes Format, das in Nessus 3.2 bis 4.0.2 verwendet wurde. Es ist kompatibel mit Nessus 4.x und Security Center 3.
Detailed HTML Report (by finding) (Detaillierter HTML-Bericht (nach Ergebnis))	Ein in Standard-HTML generierter Bericht, der in jedem Webbrowser angezeigt werden kann. Die Aufteilung erfolgt nach Sicherheitslücke (d. h. Nessus-Plugin-ID).
Detailed RTF Report (by finding) (Detaillierter RTF-Bericht (nach Ergebnis))	Ein im RTF-Format (Rich Text Format) generierter Bericht.
Executive HTML export (top 10 most vulnerable hosts) (Eingeschränkter HTML-Export (10 Hosts mit den meisten Sicherheitslücken))	Ein in Standard-HTML generierter Bericht, der nur die zehn Hosts mit den meisten Sicherheitslücken enthält.
HTML export (HTML-Export)	Ein in Standard-HTML generierter Bericht, in dem die Ergebnisse nach Hosts kategorisiert sind.
NBE export (NBE-Export)	Exportdatei mit Trennzeichen, die in viele externe Programme importiert werden kann. Als Trennzeichen kommt der Längsstrich („|“) zum Einsatz.

Copyright © 2002-2011 Tenable Network Security, Inc.

Nach Auswahl der Formate **.nessus** oder NBE wird das Standarddialogfeld „Datei speichern" Ihres Browsers angezeigt, in dem Sie die Scanergebnisse an einem Speicherort Ihrer Wahl speichern können. HTML-Berichte werden in Ihrem Browser angezeigt und können über die Browserfunktion „Datei > Speichern" gespeichert werden.

Klicken Sie zum Import eines Scans in der Liste „**Reports**" auf „**Upload**".



Klicken Sie auf die Schaltfläche „**Browse...**" („Durchsuchen"), wählen Sie die **.nessus**-Scandatei aus, die Sie importieren möchten, und klicken Sie auf „**Submit**". Nessus analysiert die Daten und macht sie über die Oberfläche „**Reports**" verfügbar.

Das .nessus-Dateiformat

Nessus verwendet zum Exportieren und Importieren ein bestimmtes Dateiformat: das **.nessus**-Format. Dieses Format bietet die folgenden Vorteile:

- Es ist XML-basiert, d. h. es bietet Aufwärts- und Abwärtskompatibilität und ist einfach zu implementieren.
- Es ist autark, d. h. die Liste der Ziele, die vom Benutzer definierten Richtlinien und die Scanergebnisse sind in einer einzigen **.nessus**-Datei enthalten.
- Es ist sicher, denn Kennwörter werden nicht in der Datei gespeichert. Stattdessen wird ein Verweis auf ein Kennwort an einem sicheren Speicherort auf dem lokalen Host abgelegt.

Der Vorgang zur Erstellung einer **.nessus**-Datei mit den Zielen, Richtlinien und Scanergebnissen beginnt mit der Erzeugung und Speicherung der Richtlinie. Danach wird die Liste mit den Zieladressen generiert und abschließend ein Scan ausgeführt. Nach Abschluss des Scans können alle Daten in einer **.nessus**-Datei gespeichert werden. Hierzu wird die Option „**Download**" auf der Registerkarte „**Reports**" verwendet. Weitere Informationen zu **.nessus**-Dateien entnehmen Sie dem Dokument „Das Nessus-Dateiformat".

Copyright © 2002-2011 Tenable Network Security, Inc.

Delete (Löschen)

Wenn Sie die Scanergebnisse nicht mehr benötigen und sie löschen möchten, wählen Sie den betreffenden Scan aus der Liste „Reports" aus und klicken auf „**Delete**". Auf diese Weise wird der Scan aus der Benutzeroberfläche gelöscht. **Dieser Vorgang kann nicht rückgängig gemacht werden!** Wenn Sie die Scanergebnisse vor dem Löschen exportieren möchten, verwenden Sie die Funktion „**Download**".

BENUTZER

Auf der Registerkarte „**Users**" („Benutzer") finden Sie Funktionen und Optionen zur Verwaltung von Benutzern des Nessus-Scanners. Neue Benutzer können über den Nessus Server Manager (Mac OS X/Windows), mithilfe des Befehls **`nessus-adduser`** (*nix) oder über die Benutzeroberfläche (alle Plattformen) hinzugefügt werden. Klicken Sie zur Erstellung eines neuen Benutzers über die Nessus-Benutzeroberfläche oben rechts im Menü auf „**Add**" („Hinzufügen"). Nun werden Sie aufgefordert, den Benutzernamen, das Kennwort und optional die Festlegung des Benutzers als Administrator für den Nessus-Scanner anzugeben:

Wählen Sie zum Bearbeiten oder Löschen eines Benutzers den Benutzernamen aus der Liste „**Users**" aus und klicken Sie oben rechts im Menü auf „**Edit**" („Bearbeiten") bzw. „**Delete**" („Löschen").

ANDERE NESSUS-CLIENTS

Zusätzlich zur Nessus-Benutzeroberfläche unterstützt Tenable zwei weitere Methoden zur Kommunikation mit dem Nessus-Server: die Befehlszeilenoberfläche und das SecurityCenter.

DIE BEFEHLSZEILENOBERFLÄCHE

Die Befehlszeilenoberfläche (auch als Command-Line Interface, kurz „CLI" bezeichnet) wird mit dem Nessus-Server zur Verfügung gestellt. Zur Ausführung eines Scans über die Befehlszeile müssen Sie diesen im Batchmodus ausführen. Hierzu wird die folgende Befehlssyntax verwendet:

Copyright © 2002-2011 Tenable Network Security, Inc.

Betriebssystem	Befehl
Linux, Solaris, Enterasys	`# /opt/nessus/bin/nessus -q [-pPS] <host> <port> <user> <password> <targets-file> <result-file>`
FreeBSD	`# /usr/local/nessus/bin/nessus -q [-pPS] <host> <port> <user> <password> <targets-file> <result-file>`
Mac OS X	`# /Library/Nessus/run/bin/nessus -q [-pPS] <host> <port> <user> <password> <targets-file> <result-file>`
Windows	`%programfiles%\Tenable\Nessus\nessus -q [-pPS] <host> <port> <user> <password> <targets-file> <result-file>`

Die nachfolgende Tabelle erläutert die verschiedenen Argumente, die zur Ausführung eines Scans im Batchmodus verwendet werden.

Argument	Beschreibung
-q	Batchmodus (Stapelverarbeitungsmodus). Führt den Nessus-Scan ohne Interaktionsmöglichkeit aus.
-p	Ruft eine Liste der auf dem Server installierten Plugins ab.
-P	Ruft eine Liste der Voreinstellungen von Server und Plugins ab.
-S	Erstellt die SQL-Ausgabe für **-p** und **-P**.
<host>	Der `nessusd`-Host, mit dem eine Verbindung hergestellt wird.
<port>	Der Port, über den Sie die Verbindung auf dem **nessusd**-Remotehost herstellen.
<user>	Benutzername, unter dem eine Verbindung mit **nessusd** hergestellt wird.
<password>	Das Kennwort zum Benutzernamen.
<targets-file>	Name der Datei, die Angaben zu den zu scannenden Zielsystemen enthält.
<results-file>	Name der Datei, in der die Ergebnisse nach Abschluss des Scans gespeichert werden.

Es gibt noch weitere Optionen, die verfügbar sind, wenn ein Scan im Batchmodus ausgeführt wird. Diese sind in der folgenden Tabelle aufgeführt.

Copyright © 2002-2011 Tenable Network Security, Inc.

Option	Beschreibung
`-V`	Zeigt im Batchmodus Statusmeldungen auf dem Bildschirm an.
`-x`	SSL-Zertifikate nicht überprüfen.
`-v`	Version. Zeigt die Versionsnummer an und wird dann beendet.
`-h`	Hilfe. Zeigt eine Befehlszusammenfassung an und wird dann beendet.
`-T <type>`	Speichert die Daten als <type>, wobei <type> („Typ") die Werte „nbe", „html", „nessus" oder „text" annehmen kann.

Bericht konvertieren

Sie können Berichte mithilfe von Nessus in ein anderes Format konvertieren. Nessus kann jeden NBE-Bericht in das HTML-, Text- oder `.nessus`-Format umwandeln.

Verwenden Sie zur Konvertierung eines Berichts folgenden Befehl:

Betriebssystem	Befehl
Linux, Solaris, Enterasys	`# /opt/nessus/bin/nessus -i in.nbe -o out.[html|txt|nessus]`
FreeBSD	`# /usr/local/nessus/bin/nessus -i in.nbe -o out.[html|txt|nessus]`
Mac OS X	`# /Library/Nessus/run/bin/nessus -i in.nbe -o out.[html|txt|nessus]`
Windows	`%programfiles%\Tenable\Nessus\nessus -i in.nbe -o out.[html|txt|nessus]`

Mit der Option `-i` wird die zu konvertierende NBE-Datei angegeben. Mit der Option `-o` legen Sie den Namen und den Typ der Datei fest, in die der Bericht konvertiert werden soll. Dies kann das HTML-, das Text- oder das `.nessus`-Format sein.

In `.nessus`-Dateien enthaltene Berichte können über die Befehlszeile auch in HTML konvertiert werden. Die hierfür erforderliche Syntax sieht wie folgt aus:

Die `.nessus`-Datei muss im Downloadformat „nessus (v1)" gespeichert sein, damit die HTML-Konvertierung gelingt.

Betriebssystem	Befehl
Linux, Solaris, Enterasys	`# /opt/nessus/bin/nessus --dot-nessus in.nessus -i <ReportName> -o out.html`

Copyright © 2002-2011 Tenable Network Security, Inc.

FreeBSD	`# /usr/local/nessus/bin/nessus --dot-nessus in.nessus -i <ReportName> -o out.html`
Mac OS X	`# /Library/Nessus/run/bin/nessus --dot-nessus in.nessus -i <ReportName> -o out.html`
Windows	`%programfiles%\Tenable\Nessus\nessus --dot-nessus in.nessus -i <ReportName> -o out.html`

Der Parameter **--dot-nessus** gibt die zu verwendende **.nessus**-Eingabedatei an. <ReportName> ist der Name des Berichts, wie er in der **.nessus**-Eingabedatei erscheint.

.nessus-Dateien auf der Befehlszeile bearbeiten

Es gibt eine Reihe von Argumenten, die übergeben werden können, um **.nessus**-Dateien als Ein- oder Ausgabe auf der Befehlszeile zu verwenden. Diese sind in der folgenden Tabelle aufgeführt:

Argument	Beschreibung
--dot-nessus <file>	Sofern verwendet, muss dieses Argument immer als erster Parameter an die **nessus**-Binärdatei übergeben werden. Hiermit wird angegeben, dass eine **.nessus**-Datei verwendet wird. <file> ist dabei der Speicherort und Name der zu verwendenden **.nessus**-Datei.
--policy-name <policy>	Der Name einer Richtlinie, die in der angegebenen **.nessus** -Datei enthalten ist. Der Richtlinienparameter wird beim Start eines Scans über die Befehlszeile angegeben. Beachten Sie, dass die Angabe des Richtliniennamens exakt erfolgen muss, d. h. einschließlich einzelner Anführungszeichen wie mit dem Parameter „**--list-policies**" angezeigt (siehe unten).
--list-policies	Gibt die Namen aller Scanrichtlinien in der angegebenen **.nessus**-Datei an.
--list-reports	Gibt die Namen aller Berichte in der angegebenen **.nessus**-Datei an.
--target-file <file>	Setzt die in der angegebenen **.nessus**-Datei enthaltenen Ziele außer Kraft und verwendet jene in der genannten Datei.

Der folgende Befehl zeigt eine Liste aller Berichte in der Datei „**scan.nessus**":

Die **.nessus**-Datei muss im Downloadformat „nessus (v1)" gespeichert sein, damit die Option **--list-reports** funktioniert.

Betriebssystem	Befehl
Linux, Solaris, Enterasys	`# /opt/nessus/bin/nessus --dot-nessus scan.nessus --list-reports`

Copyright © 2002-2011 Tenable Network Security, Inc.

FreeBSD	**# /usr/local/nessus/bin/nessus --dot-nessus scan.nessus --list-reports**
Mac OS X	**# /Library/Nessus/run/bin/nessus --dot-nessus scan.nessus --list-reports**
Windows	**%programfiles%\Tenable\Nessus\nessus --dot-nessus scan.nessus --list-reports**

Nachfolgend aufgeführt ist eine Beispielausgabe:

```
List of reports contained in scan.nessus:
- '08/03/10 11:19:55 AM - Full Safe w/ Compliance'
- '08/03/10 01:01:01 PM - Full Safe w/ Compliance'
- '08/03/10 01:32:10 PM - Full Safe w/ Compliance'
- '08/03/10 02:13:01 PM - Full Safe w/ Compliance'
- '08/03/10 02:45:00 PM - Full Safe w/ Compliance'
```

Der folgende Befehl zeigt eine Liste aller Richtlinien in der Datei „**scan.nessus**“:

Die **.nessus**-Datei muss im Downloadformat „nessus (v1)“ gespeichert sein, damit die Option **--list-policies** funktioniert.

Betriebssystem	Befehl
Linux, Solaris, Enterasys	**# /opt/nessus/bin/nessus --dot-nessus scan.nessus --list-policies**
FreeBSD	**# /usr/local/nessus/bin/nessus --dot-nessus scan.nessus --list-policies**
Mac OS X	**# /Library/Nessus/run/bin/nessus --dot-nessus scan.nessus --list-policies**
Windows	**%programfiles%\Tenable\Nessus\nessus --dot-nessus scan.nessus --list-policies**

Die Beispielausgabe dieses Befehls ist nachfolgend aufgeführt:

```
List of policies contained in scan.nessus:
- 'Full Safe w/ Compliance'
```

Beachten Sie, dass, wenn die Berichts- oder Richtliniennamen als Parameter an die Befehlszeile Nessus übergeben werden müssen, der jeweilige Name exakt so angegeben werden muss, wie er in den obigen Befehlen gezeigt ist, d. h. einschließlich der einfachen Anführungszeichen (`'Safe w/ Compliance'`).

Scanbefehl

Sofern die im obigen Beispiel angegebene Richtlinie vorhanden ist, kann ein Scan mit den folgenden Einstellungen gestartet werden:

Copyright © 2002-2011 Tenable Network Security, Inc.

Die im Scan angegebene **.nessus**-Datei muss im Format „nessus (v1)" vorliegen, damit der Scan verarbeitet wird.

Betriebssystem	Befehl
Linux, Solaris, Enterasys	`# /opt/nessus/bin/nessus --dot-nessus scan.nessus --policy-name 'Full Safe w/ Compliance' <host> <port> <user> <password> <results-file>`
FreeBSD	`# /usr/local/nessus/bin/nessus --dot-nessus scan.nessus --policy-name 'Full Safe w/ Compliance' <host> <port> <user> <password> <results-file>`
Mac OS X	`# /Library/Nessus/run/bin/nessus --dot-nessus scan.nessus --policy-name 'Full Safe w/ Compliance' <host> <port> <user> <password> <results-file>`
Windows	`%programfiles%\Tenable\Nessus\nessus --dot-nessus scan.nessus --policy-name "Full Safe w/Compliance" <host> <port> <user> <password> <results-file>`

Im obigen Beispiel wurden die Parameter **<host>**, **<port>**, **<user>**, **<password>** und **<results-file>** wie zuvor dokumentiert angegeben. Ein Parameter <targets-file> (Zieldatei) ist nicht erforderlich, da die in der **.nessus**-Datei vorhandenen Ziele für den Scan verwendet werden.

Welches Format der zu generierende Bericht hat, wird über die mit dem Befehl **nessus** übergebene Dateierweiterung festgelegt. Wäre im obigen Befehl der als <results-file> angegebene Parameter „**report.nbe**", dann würde der Bericht im **.nbe**-Format ausgegeben. Wäre der Name „**report.nessus**", dann hätte der Bericht das **.nessus**-Format.

Wäre im obigen Befehl kein Wert für den Parameter <results-file> angegeben worden, dann würde der Bericht der Datei **scan.nessus** hinzugefügt.

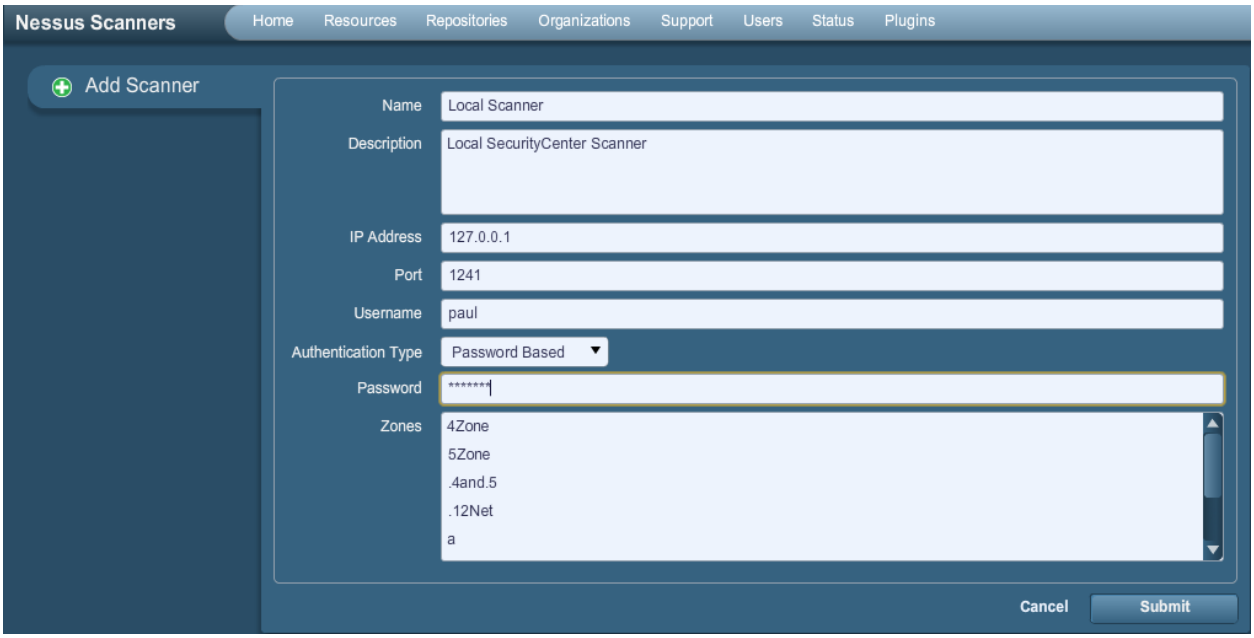
SECURITYCENTER

SecurityCenter konfigurieren

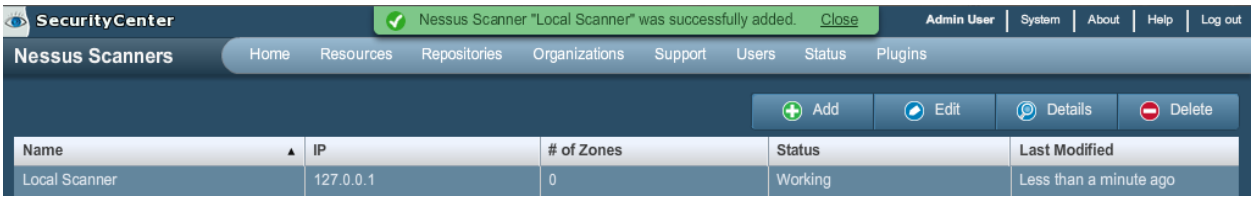
Ein Nessus-Server kann über die SecurityCenter-Verwaltungsoberfläche hinzugefügt werden. Mithilfe dieser Oberfläche lässt sich SecurityCenter so konfigurieren, dass von hier aus auf praktisch jeden Nessus-Scanner zugegriffen und dieser gesteuert werden kann. Klicken Sie auf die Registerkarte „Resources" („Ressourcen") und dann auf „**Nessus Scanners**". Klicken Sie auf „**Add**" („Hinzufügen"), um das Dialogfeld „Add Scanner" („Scanner hinzufügen") zu öffnen. Angegeben werden müssen die IP-Adresse des Nessus-Scanners, der Nessus-Port (Standard: 1241), der Anmeldename des Administrators, der Authentifizierungstyp und das (bei der Konfiguration von Nessus erstellte) Kennwort. Die Kennwortfelder sind nicht verfügbar, wenn die Authentifizierung via SSL-Zertifikat (Option „SSL Certificate") ausgewählt wird. Außerdem können unter „Zones" Zonen festgelegt werden, denen der Nessus-Scanner zugeordnet werden kann.

Nachfolgend gezeigt ist eine Bildschirmabbildung der SecurityCenter-Seite „Add Scanner":

Copyright © 2002-2011 Tenable Network Security, Inc.



Nach dem erfolgreichen Hinzufügen des Scanners wird die folgende Seite angezeigt:



Weitere Informationen finden Sie im „SecurityCenter-Administrationshandbuch".

WEITERE INFORMATIONEN

Tenable hat eine Reihe von Dokumenten erstellt, in denen die Installation, Bereitstellung, Konfiguration, der Betrieb und die Testmethoden von Nessus ausführlich beschrieben werden. Es sind diese:

- **Nessus-Installationshandbuch** (Schrittanleitung zur Nessus-Installation)
- **Authentifizierte Nessus-Tests für UNIX und Windows** (enthält Informationen zur Durchführung authentifizierter Netzwerkscans mit dem Nessus-Sicherheitslückenscanner)
- **Nessus-Compliancetests** (allgemeiner Leitfaden zum Verständnis und zur Durchführung von Compliancetests mithilfe von Nessus und SecurityCenter)
- **Nessus-Referenzhandbuch für Compliancetests** (umfassender Leitfaden zur Syntax von Nessus-Compliancetests)
- **Nessus V2-Dateiformat** (beschreibt die Struktur des `.nessus`-Dateiformats, das mit Nessus 3.2 und NessusClient 3.2 eingeführt wurde)
- **Nessus XML-RPC-Protokollspezifikation** (beschreibt das XML-RPC-Protokoll und die Schnittstelle in Nessus)

Copyright © 2002-2011 Tenable Network Security, Inc.

- **Compliance-Überwachung in Echtzeit** (erläutert, wie die Lösungen von Tenable Sie bei der Erfüllung zahlreicher gesetzlicher Vorschriften und Finanzstandards unterstützt)

Setzen Sie sich mit uns in Verbindung – via E-Mail (support@tenable.com, sales@tenable.com) oder über unsere Website unter http://www.tenable.com/.

Copyright © 2002-2011 Tenable Network Security, Inc.

WISSENSWERTES ZU TENABLE NETWORK SECURITY

Tenable Network Security gehört zu den Marktführern im Bereich Unified Security Monitoring. Das Unternehmen entwickelt den Nessus-Sicherheitslückenscanner und bietet agentenlose Unternehmenslösungen für die fortlaufende Überwachung auf Sicherheitslücken, Konfigurationsfehler, Datenlecks, Protokollverwaltung und Risikoerkennung an, um die Sicherheit im Netzwerk und die Compliance in Bezug auf Standards wie FDCC, FISMA, SANS CAG und PCI sicherzustellen. Die preisgekrönten Produkte von Tenable werden von zahlreichen Global 2000-Unternehmen und staatlichen Einrichtungen in aller Welt verwendet, um Risiken im Netzwerk proaktiv zu minimieren. Weitere Informationen finden Sie unter http://www.tenable.com/.

Tenable Network Security, Inc.
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046, USA
410.872.0555
www.tenable.com

Copyright © 2002-2011 Tenable Network Security, Inc.